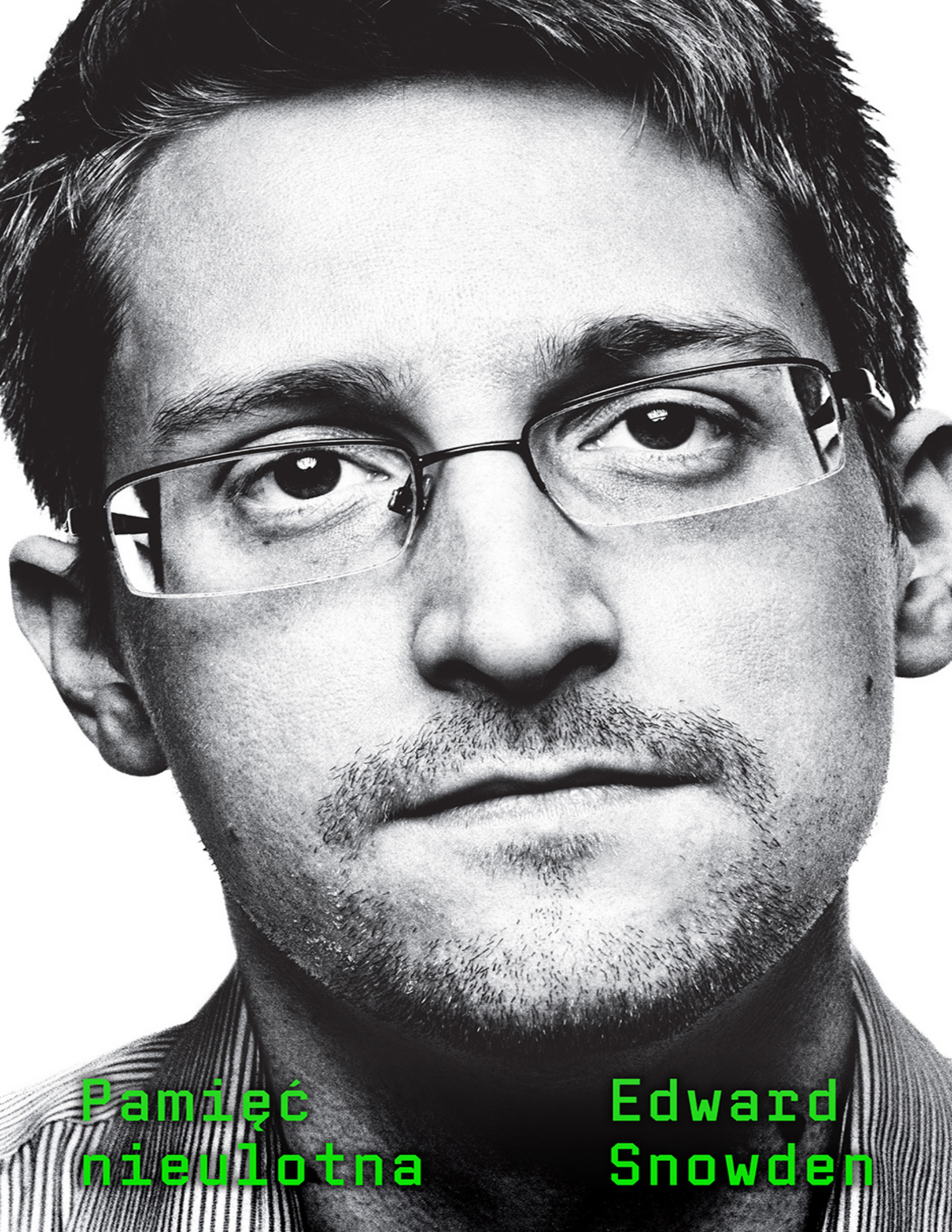
Pamięć
nieulotna
Edward
Snowden

Edward Snowden

PAMIĘĆ NIEULOTNA

przekład
Michał Jóźwiak
Michał Strąkow
oraz
Bożena Jóźwiak

insignis

Tytuł oryginału
Permanent Record

First published by Metropolitan Books
Henry Holt and Company, LLC
Publisher since 1886
120 Broadway, New York, NY 10271
www.henryholt.com

Copyright © 2019 by Edward Snowden
All rights reserved.

Przekład
Michał Jóźwiak (rozdziały: 0–2, 6–7, 10–12, 15–16, 20, 23–24, 26, 27),
Michał Strąkow (rozdziały: 3–5, 8–9, 13–14, 17–18, 22, 29),
Bożena Jóźwiak (rozdziały: 19, 21, 25, 27, 28, Podziękowania)

Redakcja
Tomasz Brzozowski, Monika Skowron

Korekta
Małgorzata Kłosowicz

Projekt okładki
Rodrigo Corral

Zdjęcie autora
© Platon

Skład
Tomasz Brzozowski

Konwersja do wersji elektronicznej
Aleksandra Pieńkosz

Copyright © for this edition Insignis Media, Kraków 2019
Wszelkie prawa zastrzeżone.

ISBN 978-83-66360-25-9

Insignis Media
ul. Lubicz 17D/21–22, 31-503 Kraków

tel. +48 (12) 636 01 90
biuro@insignis.pl, www.insignis.pl
facebook.com/Wydawnictwo.Insignis
twitter.com/insignis_media (@insignis_media)
instagram.com/insignis_media (@insignis_media)
Snapchat: insignis_media

Dla_L.|

Dokument chroniony elektronicznym znakiem wodnym

Zakupione w nexto: 3043996

00_Przedmowa|

Nazywam się Edward Snowden. Kiedyś byłem agentem rządowym, teraz jednak działam na rzecz obywateli. Potrzebowałem prawie trzech dekad, by zdać sobie sprawę, że jedno i drugie to nie to samo, a kiedy dostrzegłem różnicę, narobiłem sobie kłopotów u pracodawcy. W rezultacie obecnie poświęcam swój czas na chronienie społeczeństwa przed takimi jak ja: szpiegami Centralnej Agencji Wywiadowczej (Central Intelligence Agency, CIA) i Agencji Bezpieczeństwa Narodowego (National Security Agency, NSA), młodymi ludźmi o technicznym wykształceniu, starającymi się budować świat, który w ich przekonaniu będzie lepszy.

Moja kariera w amerykańskich służbach wywiadowczych trwała jedyne siedem lat, czyli – co stwierdzam z pewnym zaskoczeniem – tylko rok dłużej niż moje życie na wygnaniu w kraju, którego nie wybrałem. Na przestrzeni tych siedmiu lat miałem jednak okazję brać udział w jednym z najważniejszych przełomów w historii amerykańskiego wywiadu – odejściu od śledzenia pojedynczych osób na rzecz masowej inwigilacji całych społeczeństw. Przyłożyłem rękę do powstania technologii, która umożliwiła rządowi jednego państwa gromadzenie przekazów cyfrowych z całego świata, przechowywanie ich całymi latami, a także przeszukiwanie tych zasobów, kiedy tylko zajdzie potrzeba.

Po wydarzeniach z 11 września 2001 roku amerykańskie służby wywiadowcze ogarnęło druzgocące poczucie winy, że nie zdołały zapewnić Ameryce bezpieczeństwa i dopuściły do najbardziej niszczycielskiego ataku na nasz kraj od czasu Pearl Harbor. Przywódcy tych służb postanowili zatem stworzyć system, który miał zapobiec podobnej sytuacji w przyszłości. U jego podstaw miała lec nowoczesna technologia, rzecz obca armii politologów i magistrów zarządzania, stanowiącej trzon wywiadu. Dlatego wszystkie najbardziej tajne agencje otworzyły szeroko drzwi młodym adeptom technologii – takim jak ja. Geeki na własność posiadły ziemię.

Komputery były jedyną rzeczą, na której w tamtych czasach znałem się dobrze, dzięki czemu szybko piąłem się w hierarchii. Miałem dwadzieścia dwa lata, kiedy otrzymałem pierwszy dostęp kategorii „ściśle tajne” i objąłem stanowisko na najniższym szczeblu struktury NSA. Niecały rok później pracowałem już dla CIA w roli projektanta systemów informatycznych ze swobodnym dostępem do kilku spośród najbardziej poufnych sieci na naszej planecie. Nadzór kierownictwa ograniczał się tylko do tego, że towarzyszył mi facet, który zabijał czas, czytając na swojej zmianie powieści Roberta Ludluma i Toma Clancy’ego.

Agencje postawiły sobie za cel jak najszybsze pozyskanie utalentowanych informatyków i żeby go osiągnąć, łamały wszystkie wewnętrzne zasady. Wcześniej za żadne skarby nie zatrudniłyby nikogo, kto nie miał ukończonych studiów magisterskich albo chociaż licencjackich. Ja nie mogłem się pochwalić ani jednym, ani drugim. Gdyby obowiązywały normalne reguły, nigdy nie postawiłbym swojej stopy na terenie placówki wywiadowczej.

W latach 2007–2009 pracowałem w ambasadzie amerykańskiej w Genewie jako jeden z nielicznych informatyków działających pod

przykrywką dyplomatyczną. Moim zadaniem było przenieść CIA w przyszłość poprzez cyfryzację i automatyzację sieci, którą rząd Stanów Zjednoczonych wykorzystywał do celów wywiadowczych, oraz włączenie w nią europejskich placówek agencji. Moje pokolenie nie tyle przeprojektowało działanie służb wywiadowczych, ile je zupełnie przedefiniowało. Nie interesowały nas tajne spotkania ani zostawianie sobie nawzajem przedmiotów w tajnych skrytkach. Dla nas liczyły się tylko dane.

W wieku dwudziestu sześciu lat byłem oficjalnie pracownikiem Della, a w praktyce ponownie agentem NSA. Moją przykrywką, podobnie jak większości technologicznie uzdolnionych szpiegów mojego pokolenia, stały się zlecenia kontraktowe. Wysłano mnie do Japonii, gdzie pomogłem zaprojektować system pełniący zasadniczo rolę globalnej kopii zapasowej danych NSA – gigantyczną tajną sieć, która zapewniała, że nawet gdyby wybuch nuklearny zrównał z ziemią siedzibę główną agencji, nie doszłoby do utraty żadnych informacji. Wówczas nie zdawałem sobie jeszcze sprawy, że stworzenie systemu trwale dokumentującego życie wszystkich ludzi na świecie było tragicznym błędem.

Kiedy wróciłem do Stanów, miałem dwadzieścia osiem lat i otrzymałem niebotyczny awans – trafiłem do zespołu, którego zadaniem była koordynacja współpracy pomiędzy Dellem a CIA. Moje zadanie polegało na spotykaniu się z szefami działów technologicznych CIA, opracowywaniu rozwiązań wszelkich problemów, które przychodziły im do głowy, i przekonywaniu ich, by te rozwiązania wdrożyli. Mój zespół pomógł agencji zbudować nowy rodzaj architektury przetwarzania danych – „chmurę” – pierwszą technologię, która dawała wszystkim agentom, niezależnie od miejsca, w którym się fizycznie znajdowali, dostęp do wszelkich potrzebnych informacji i możliwość ich przeszukiwania.

Podsumowując, praca wywiadowcza, która początkowo polegała na łączeniu kanałów informacji, ustąpiła miejsca szukaniu sposobu, jak zachować te dane na zawsze, a następnie zapewnić ich globalną dostępność i możliwość przeszukiwania. Sens projektów, którymi się zajmowałem, zaczął do mnie docierać dopiero wtedy, kiedy w wieku dwudziestu dziewięciu lat przeprowadziłem się na Hawaje, by podjąć się kolejnego zlecenia dla NSA. Wcześniej pracowałem zgodnie z doktryną *Need to Know* („co potrzebujesz wiedzieć") – otrzymywałem wytyczne potrzebne wyłącznie do realizacji bieżących zadań. Dopiero kiedy znalazłem się w informacyjnym raju, pojąłem łączne znaczenie moich specjalistycznych projektów i dostrzegłem, jak efekty mojej pracy zazębiają się niczym tryby potężnej machiny napędzającej system globalnej inwigilacji.

W tunelu ukrytym głęboko pod polem ananasów, stanowiącym część dawnej podziemnej fabryki samolotów z czasów Pearl Harbor, siedziałem przed terminalem. Dawał mi on praktycznie nieograniczony dostęp do komunikacji niemal każdej osoby dowolnej płci i w obojętnie jakim wieku, która kiedykolwiek skorzystała z telefonu albo miała kontakt z komputerem. Wśród nich było około 320 milionów moich rodaków, których codzienne życie rejestrowano, rażąco łamiąc nie tylko zapisy Konstytucji Stanów Zjednoczonych, ale i podstawowe wartości każdego wolnego społeczeństwa.

Czytasz tę książkę, bo dokonałem rzeczy niebezpiecznej dla osoby na moim stanowisku: zdecydowałem się powiedzieć prawdę. Zgromadziłem wewnętrzne dokumenty wywiadu dowodzące łamania prawa przez rząd Stanów Zjednoczonych i przekazałem je dziennikarzom, oni zaś potwierdzili ich autentyczność, a następnie opublikowali, czym wywołali światowy skandal.

Książka ta opowiada o zdarzeniach poprzedzających moją decyzję, o zasadach moralnych i etycznych, które do niej doprowadziły, i o źródle tych zasad. A zatem jest to książka również o moim życiu.

Co składa się na życie? Więcej, niż mówimy. Więcej, nawet niż robimy. Życie to również wszystko, co kochamy, oraz wartości, jakie wyznajemy. Dla mnie tym, co kocham i w co wierzę najmocniej, są więzi międzyludzkie i technologie, dzięki którym te więzi są budowane. Wśród tych technologii znajdują się, rzecz jasna, książki. Jednak dla mojego pokolenia głównym narzędziem kultywowania więzi międzyludzkich stał się internet.

Zanim dopadną cię mdłości na myśl o toksycznym szaleństwie, którym zainfekowany jest współczesny sieciowy ul, zrozum, że kiedy ja poznałem internet, wyglądał zupełnie inaczej. Był przyjacielem i rodzicem. Społecznością bez granic i barier; głosem w równej mierze jednostek, co milionów; otwartym na wszystkich Dzikim Zachodem; przestrzenią, gdzie osiedliły się bez wyzyskiwania kogokolwiek najróżniejsze plemiona, by żyć obok siebie i gwarantować swoim członkom swobodny wybór imion, historii i zwyczajów. Wszyscy nosili maski, a mimo to kultura tej anonimowości osiąganej pseudonimizacją* generowała więcej prawdy niż fałszu – stawiała na kreatywność i współpracę, a nie na komercję i współzawodnictwo. Nie był jej obcy konflikt, oczywiście, ale przeważały dobre intencje i pozytywne uczucia. Przepełniał ją prawdziwy pionierski duch.

Zrozumiesz zatem, co mam na myśli, pisząc, że nie poznaję dzisiejszego internetu. Warto przy okazji podkreślić, że zmiana, która nastąpiła, była skutkiem świadomego systematycznego działania garstki uprzywilejowanych. Pęd do przekształcenia biznesu w e-biznes, który towarzyszył wczesnemu internetowi, szybko doprowadził do powstania

bańki, a później, na początku XXI wieku, do załamania rynku. Firmy wyciągnęły z tego naukę. Zdały sobie sprawę, że użytkownicy sieci od wydawania pieniędzy zdecydowanie wolą dzielenie się własnym życiem, a więzi międzyludzkie, które budują w internecie, można spieniężyć. Skoro ludzie chcą wykorzystywać sieć przede wszystkim po to, by informować rodzinę, przyjaciół, a nawet nieznajomych, co się u nich dzieje, i otrzymywać od nich w zamian podobne informacje, przedsiębiorstwa musiały jedynie znaleźć sposób, by stać się pośrednikiem wszystkich tych wymian społecznych i przekuć je w dochód.

Ten tok myślenia dał początek kapitalizmowi inwigilacyjnemu i zakończył żywot internetu, który znałem.

W nowej rzeczywistości kreatywny aspekt sieci praktycznie zanikł – niezliczone piękne, trudne, indywidualistyczne strony internetowe zamknęły swoje podwoje. Obietnica wygody przekonała użytkowników, by wymienili osobiste witryny, które wymagały ciągłej uwagi i pracochłonnych zabiegów, na profil na Facebooku i konto Gmail. Bardzo łatwo można było ulec złudzeniu posiadania ich na własność. Mało kto dostrzegał to już wtedy, ale wszystko, czym dzielimy się w sieci, miało przestać należeć do nas. Nowe firmy e-commerce – sukcesorki tych, które upadły, ponieważ nie potrafiły znaleźć niczego, co chcielibyśmy kupić – zaczęły sprzedawać nowy produkt.

Byliśmy nim my.

Nasza uwaga, nasze zajęcia, nasze pragnienia – wszystko, co na swój temat zdradziliśmy, świadomie bądź nie – było rejestrowane i sprzedawane. Potajemnie, by odsunąć w czasie nieuniknione poczucie naruszenia prywatności, które większości z nas zaczęło doskwierać dopiero teraz. Co gorsza, inwigilacja ta zyskała aktywne poparcie, a nawet finansowanie od całej armii rządów łasej na olbrzymie banki danych wywiadowczych, które

w ten sposób mogła pozyskać. Zważywszy, że w pierwszych latach XXI wieku większość komunikacji internetowej, poza loginami i transakcjami finansowymi, nie była szyfrowana, w wielu przypadkach rządy nie musiały w ogóle kontaktować się z korporacjami, by wiedzieć, co robią ich klienci. Mogły szpiegować świat, nie puszczając pary z ust.

Rząd amerykański całkowicie lekceważąc postanowienia aktu założycielskiego swojego państwa, uległ tej właśnie pokusie, a kiedy skosztował owocu z zatrutego drzewa, rozgorzał nieuleczalną gorączką. W tajemnicy dał sobie przyzwolenie na masową inwigilację – formę władzy z definicji dotykającą o wiele mocniej niewinnych niż przestępców.

Dopiero kiedy pełniej zdałem sobie sprawę z istnienia systemu inwigilacji i powiązanych z nim zagrożeń, zaczęła trapić mnie świadomość, że nam, członkom społeczeństwa – nie tylko amerykańskiego, ale i światowego – w ogóle nie było dane zagłosować czy choćby wyrazić opinię w tej sprawie. Rząd uruchomił system niemal powszechnej inwigilacji nie dość, że bez naszej zgody, to jeszcze świadomie w taki sposób, by ukryć przed nami prawdę o wszystkich programach. Na każdym kroku zmiany w procedurach oraz ich konsekwencje były starannie ukrywane, również przed większością prawodawców. Do kogo mogłem się zwrócić? Z kim porozmawiać na ten temat? Rząd zadbał, by najcichszy szept prawdy, przedstawienie podstawowych faktów w najmożliwiej ogólnikowy sposób, nawet sędziemu, prawnikowi czy przed Kongresem, stało się tak poważnym przestępstwem, że groziło spędzeniem reszty życia za kratami federalnego więzienia.

Poczułem się zagubiony i na czas zmagań z sumieniem wpadłem w podły nastrój. Kocham swój kraj i wierzę w służbę publiczną. Wśród moich przodków pełno jest mężczyzn i kobiet, którzy służyli naszemu państwu i jego obywatelom. Sam również przysięgałem – nie przed

agencją, a nawet nie przed rządem, lecz przed narodem – działać na rzecz i w obronie konstytucji gwarantującej te same swobody obywatelskie, które zostały tak rażąco pogwałcone. Pogwałcone, niestety, między innymi przeze mnie. Dla kogo pracowałem przez wszystkie te lata? Jak miałem pogodzić obowiązek dyskrecji, wynikający z zatrudnienia przez agencje wywiadowcze, z przysięgą wierności ideałom założycielskim własnego kraju? Komu – i czemu – winien byłem większą lojalność? Kiedy powinienem poczuć się moralnie zobligowany do złamania prawa?

Rozważania nad tymi pytaniami przyniosły w końcu odpowiedzi, których potrzebowałem. Zdałem sobie sprawę, że nawiązanie kontaktu z dziennikarzami i wyjawienie im skali nadużyć, jakich dopuściło się moje państwo, nie będzie tym samym, co namawianie do radykalnych działań takich jak obalenie rządu albo delegalizacja działań wywiadowczych. Zależało mi wyłącznie na tym, by rząd i wywiad zaczęły z powrotem postępować zgodnie z ideałami, którymi się afiszowały.

Jedyną miarą wolności kraju jest stopień poszanowania praw obywatelskich. W moim przekonaniu prawa te są w rzeczywistości ograniczeniami władzy państwowej; określają konkretne ramy, w których rządowi nie wolno naruszać swobód osobistych – domenę w czasach rewolucji amerykańskiej noszącą miano wolności, a w dobie rewolucji internetowej rozumianą jako prywatność.

Minęło sześć lat od chwili, gdy się ujawniłem. Zrobiłem to, ponieważ stałem się świadkiem słabnącego zaangażowania rządów tak zwanych krajów rozwiniętych w ochronę prywatności, którą uważam – podobnie jak Organizacja Narodów Zjednoczonych – za fundamentalne prawo człowieka. Niestety na przestrzeni tego czasu zaangażowanie to osłabło jeszcze bardziej, bo w krajach demokratycznych nastąpił skręt w stronę

populistycznego autorytaryzmu. Regres uwidocznił się najsilniej w relacjach pomiędzy rządzącymi a prasą.

Próbom podkopania autorytetu dziennikarstwa podejmowanym przez demokratycznie wybranych reprezentantów społeczeństwa towarzyszy bezpardonowa kampania wymierzona w fundamenty prawdy. Prawdziwe przekazy celowo miesza się z fałszywymi, wykorzystując technologię zdolną generować zamęt na niespotykaną dotąd globalną skalę.

Znam ten proces od podszewki, ponieważ tworzenie alternatywnej rzeczywistości to najmroczniejsza ze sztuk uprawianych przez wywiad. Agencje, które na przestrzeni mojej krótkiej kariery sfabrykowały pretekst do wojny, manipulując informacjami wywiadowczymi, i poprzez nielegalne działania oraz tajne sądy zapewniły sobie prawo do porwań („transferów nadzwyczajnych”), tortur („wzmocnionych technik przesłuchań”) i powszechnej inwigilacji („masowego gromadzenia danych”), bez zwłoki przypięły mi łatę chińskiego podwójnego agenta, rosyjskiego potrójnego, a nawet, o zgrozo, milenialsa.

Udało im się powiedzieć na mój temat tak wiele i z taką swobodą, ponieważ zdecydowałem, że nie będę się bronił. Od chwili, gdy wyjawiłem swoją tożsamość, trzymałem się postanowienia, by nie ujawniać żadnych szczegółów z życia osobistego, które mogłyby skazać na jeszcze większe nieprzyjemności znajomych oraz członków rodziny, i tak cierpiących już w imię moich zasad.

Obawa, że sprowadzę na kogoś jeszcze większe kłopoty, była przyczyną wielu rozterek przed napisaniem tej książki. W ostatecznym rozrachunku decyzja, by przekazać dziennikarzom dowody nielegalnego postępowania rządu, sprawiła mi mniej trudu niż ta, by opowiedzieć o swoim życiu. Nadużycia, których byłem świadkiem, wymagały reakcji, nikt jednak nie decyduje się na spisanie wspomnień tylko dlatego, że nie potrafi oprzeć się

nakazowi sumienia. Z tego powodu postarałem się o zgodę wszystkich członków rodziny, znajomych i dawnych współpracowników, których przedstawiam na stronach mojej książki z nazwiska bądź w inny sposób zdradzający ich tożsamość.

Podobnie jak nie zamierzam samodzielnie decydować o cudzej prywatności, tak od początku zakładałem, że nie będę na własną rękę wybierał, jakie tajemnice mojego kraju upublicznić, a jakich nie. Dlatego ujawniłem rządowe dokumenty wyłącznie dziennikarzom. Liczba dokumentów, które podałem do wiadomości opinii publicznej, wynosi zero.

Uważam, podobnie jak wspomniani dziennikarze, że nie ma nic złego w ukrywaniu pewnych informacji przez rząd. Nawet najbardziej transparentna demokracja świata powinna mieć prawo do ochrony – na przykład – tożsamości tajnych agentów i ruchów swoich wojsk. Ta książka nie zawiera ani jednej tajemnicy takiej natury.

Opowiedzieć historię mojego życia, chroniąc prywatność moich najbliższych i nie wyjawiając tajemnic rządowych, które rzeczywiście powinny pozostać nieznane, to niełatwe zadanie, ale muszę się go podjąć. I skoro przyszło mi zmierzyć się z tymi dwoma ograniczeniami, odnajdziesz prawdę o mnie w przestrzeni pomiędzy nimi.

---

* Przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie bez użycia dodatkowych informacji (przyp. red.).

Część_01|

01_Widok_z_okna|

Pierwszym, co zhakowałem, była godzina pójścia do łóżka.

Uważałem za niegodziwe, że rodzice zmuszają mnie, bym kładł się spać wcześniej od nich i mojej siostry, choć jeszcze nie byłem zmęczony. Taka pierwsza drobna niesprawiedliwość, której doświadczyłem.

Wiele spośród mniej więcej pierwszych dwóch tysięcy nocy mojego życia kończyło się aktami nieposłuszeństwa obywatelskiego, aż w noc numer 2139 – noc moich szóstych urodzin – nareszcie odkryłem moc bezpośredniego działania. Organy władzy puszczały mimo uszu moje nawoływania do reform, a ja nie należałem do naiwniaków. Dopiero co spędziłem jeden z najprzyjemniejszych dni mojego krótkiego życia – odwiedzili mnie przyjaciele, było przyjęcie, nawet prezenty – i nie zamierzałem pozwolić, by się skończył tylko dlatego, że wszyscy musieli wrócić do siebie. Potajemnie cofnąłem zatem wszystkie zegary w domu o kilka godzin. Z zegarem mikrofalówki poradziłem sobie szybciej niż z tym na piekarniku, głównie dlatego, że było mi łatwiej do niego dosięgnąć.

Kiedy siły wyższe w swej nieskończonej ignorancji nie zwróciły uwagi, co zrobiłem, upoiłem się władzą i zacząłem galopować wokół salonu. Ja, władca czasu, miałem już nigdy nie zostać wysłany do łóżka. Byłem wolny. I w ten oto sposób spowodowałem, że niedługo po tym, jak ujrzałem najpóźniejszy w roku zachód słońca – był to dzień przesilenia letniego – zasnąłem na podłodze. Kiedy się obudziłem, zegary w domu z powrotem pokazywały czas zgodny z zegarkiem taty.

Względem czego nastawiłby dziś swój zegarek ktoś, kto chciałby zrobić to ręcznie? Jeśli postępujesz jak większość ludzi, przyjąłbyś za wzorzec czas na swoim smartfonie. Gdybyś jednak przyjrzał się mu naprawdę uważnie i zagłębił się w jego ustawienia, w końcu odkryłbyś, że jego zegar jest „ustawiany automatycznie". Co pewien czas twój telefon w tajemnicy – bezgłośnie – pyta sieć operatora: „Hej, która godzina?". Sieć operatora z kolei zadaje to samo pytanie innej sieci, większej, ta jeszcze większej, i tak dalej, poprzez długi szereg wież transmisyjnych i kabli, aż zapytanie dotrze do jednego z prawdziwych władców czasu, serwera NTP (Network Time Protocol, protokołu synchronizacji czasu), bezpośrednio sprzężonego bądź korygującego swoje nastawy z zegarami atomowymi znajdującymi się między innymi w Narodowym Instytucie Standaryzacji i Technologii w Stanach Zjednoczonych, Federalnym Instytucie Meteorologii i Klimatologii w Szwajcarii oraz w Narodowym Instytucie Technologii Informacyjnych i Komunikacyjnych w Japonii. Tej długiej niewidocznej podróży, która odbywa się w ułamku sekundy, zawdzięczasz to, że za każdym razem, gdy włączasz telefon po rozładowaniu baterii, jego zegar nie pokazuje mrugającej godziny 12:00.

Urodziłem się w 1983 roku, u schyłku świata, w którym ludzie sami nastawiali sobie zegarki. Tego samego roku Departament Obrony Stanów Zjednoczonych rozdzielił swój wewnętrzny system połączonych komputerów na dwie sieci: jedną o nazwie MILNET i przeznaczoną do użytku sił obronnych oraz drugą, publiczną – jej nadano nazwę Internet. Do końca tego samego roku powstały zasady wytyczające granice tej wirtualnej przestrzeni i dające początek wykorzystywanemu do dziś systemowi nazw domen – końcówek .gov, .mil, .edu i, rzecz jasna, .com – oraz kodów przydzielonych pozostałym państwom: .uk, .de, .fr, .cn, .ru i tak dalej. Zatem już na tym etapie mój kraj miał przewagę (a co za tym idzie – ja też).

Musiało jednak minąć sześć lat, zanim wynaleziono sieć World Wide Web, i kolejne trzy, nim moja rodzina weszła w posiadanie komputera z modemem, który mógł się połączyć z siecią.

Mamy w zwyczaju wypowiadać się o internecie, jakby był jednolitym tworem, ale, rzecz jasna, tak nie jest. Od strony technicznej rzeczywistość wygląda w ten sposób, że każdego dnia w globalnym klastrze połączonych sieci komunikacyjnych, z którego korzystasz regularnie wraz z trzema miliardami innych osób, czy też mniej więcej czterdziestoma dwoma procentami populacji świata, rodzą się nowe sieci. Mimo to będę używał słowa internet w najszerszym znaczeniu: jako określenia powszechnej sieci złożonej z innych, łączącej większość komputerów na świecie za pośrednictwem szeregu wspólnych protokołów.

Prawdopodobnie zacząłeś się niepokoić, słysząc o protokołach, bo nie masz zielonego pojęcia, czym są, ale niepotrzebnie, bo wszyscy z nich korzystamy. Możesz myśleć o nich jak o językach komunikowania się maszyn – wspólnych zasadach, do których stosują się urządzenia, by rozumieć się nawzajem. Jeśli jesteś mniej więcej w moim wieku, prawdopodobnie pamiętasz, że kiedyś, wpisując adres strony internetowej w pasek przeglądarki, należało zacząć od liter „http”. Było to odniesienie do protokołu przesyłania dokumentów hipertekstowych HTTP (Hypertext Transfer Protocol) – języka łączącego cię z siecią World Wide Web, czyli ogromnym zbiorem stron, w większości opartych na tekście, ale zdolnych również do obsługi zawartości audio/wideo, takich jak Google, YouTube i Facebook. Za każdym razem, gdy sprawdzasz skrzynkę e-mail, wykorzystujesz język IMAP (Internet Message Access Protocol, internetowy protokół dostępu do wiadomości), SMTP (Simple Mail Transfer Protocol, prosty protokół przekazywania poczty) albo POP3 (Post Office Protocol, protokół węzłów pocztowych). Pliki przedostają się przez

internet za pośrednictwem protokołu FTP (File Transfer Protocol, protokół przekazywania plików). Jeśli zaś chodzi o procedurę ustalania czasu przez smartfona, o której wspominałem, to aktualizacje docierają na twoje urządzenie przez NTP.

To wszystko to tak zwane protokoły warstwy aplikacji, które składają się na jedną z niezliczonych rodzin protokołów internetowych. Przykładowo, by dane przekazywane w którymkolwiek spośród protokołów, które właśnie wymieniłem, mogły przepłynąć internet i dotrzeć na twój komputer stacjonarny, laptop albo telefon, muszą zostać spakowane w specjalistyczny protokół transportowy. Obowiązuje tu podobna zasada, co na tradycyjnej poczcie, która preferuje, by wysyłać listy i paczki w znormalizowanych kopertach i kartonach. Protokół transportowy TCP (Transmission Control Protocol, protokół kontroli transmisji) jest wykorzystywany między innymi do przesyłania stron internetowych i maili. Z kolei w wypadku aplikacji działających w czasie rzeczywistym, na przykład w telefonii internetowej i streamingu na żywo, stosuje się protokół UDP (User Datagram Protocol, protokół datagramów użytkownika).

Każda próba przedstawienia wielowarstwowej natury tworu nazywanego w moim dzieciństwie cyberprzestrzenią, siecią, netem i autostradą informacyjną, jest skazana na niekompletność, ale warto zapamiętać jedną rzecz: protokoły, które wymieniłem, dały nam możliwość umieszczania w sieci niemal wszystkiego, czego nie jemy, nie pijemy, w co się nie ubieramy i w czym nie mieszkamy. Internet stał się prawie tak samo nieodzowną częścią naszego życia, co powietrze, przez które podróżuje większa część naszych przekazów. I – jak przypominamy sobie przy każdym powiadomieniu z mediów społecznościowych o pojawieniu się kompromitującego wpisu, w którym nas otagowano – wszystko, czemu

nadaje się formę cyfrową, zostaje zapisane w formacie, który przetrwa na zawsze.

Kiedy wspominam swoje dzieciństwo, a przede wszystkim pierwsze dziewięć lat bez internetu, uderza mnie zawsze pewna obserwacja: nie potrafię odtworzyć wszystkiego, co się wtedy działo, bo mogę polegać tylko na swojej pamięci. Dane z tego okresu po prostu nie istnieją. Kiedy byłem dzieckiem, wyrażenie „niezapomniane przeżycie” nie było jeszcze złowrogo brzmiącą, dosłowną techniczną definicją, lecz emocjonalnie nacechowanym określeniem takich zdarzeń, jak moje pierwsze słowa, pierwsze kroki, pierwszy ząb, który mi wypadł, czy pierwsza przejażdżka na rowerze.

Moje pokolenie było ostatnim w historii Ameryki, a prawdopodobnie i świata, o którym można to powiedzieć; byliśmy ostatnim niezdigitalizowanym pokoleniem z dzieciństwem niezapisanym w chmurze, lecz w dużej mierze utrwalonym w formatach analogowych, takich jak odręcznie pisane pamiętniki, zdjęcia polaroidowe i kasety VHS, namacalne i niedoskonałe artefakty, które ulegają degradacji wraz z upływem czasu i mogą zostać bezpowrotnie utracone. Odrabiałem zadania domowe na papierze przy pomocy ołówka i gumki, a nie na połączonym z siecią tablecie rejestrującym dotknięcia klawiszy. Za dokumentację skoków mojego wzrostu nie odpowiadały technologie inteligentnego budynku, lecz framuga drzwi w domu rodzinnym, gdzie rodzice zaznaczali kreski nożem.

Mieszkaliśmy w imponującym starym domu z czerwonej cegły; okalał go nieduży trawnik zacieniony przez derenie, a latem upstrzony kwiatami magnolii służącymi za osłonę plastikowym żołnierzykom, którymi się tam bawiłem. Dom miał nietypowy układ: drzwi wejściowe znajdowały się na pierwszym piętrze i prowadziły do nich masywne ceglane schody. Na tej

kondygnacji mieściła się główna przestrzeń mieszkalna: kuchnia, salon i sypialnie.

Piętro wyżej znajdował się zakurzony, pełen pajęczyn, zakazany strych, nawiedzany, jeśli wierzyć mojej mamie, przez wiewiórki czy też, jak upierał się mój tato, przez wampiry-wilkołaki, które pożerały każde dziecko na tyle niemądre, by się tam zapuścić. Pod kondygnacją mieszkalną mieściła się z kolei z grubsza wykończona piwnica – rzecz w Karolinie Północnej rzadko spotykana, szczególnie tak blisko wybrzeża, bo podpiwniczenia mają to do siebie, że często zbiera się w nich woda. Nasze niewątpliwie przez cały rok było zawilgocone, mimo działających na okrągło osuszacza powietrza i pompy drenażowej.

Kiedy moja rodzina się wprowadzała, powiększyła piętro mieszkalne o dobudówkę, gdzie znalazły się pralnia, łazienka, mój pokój oraz salon z telewizorem i kanapą. Na ten ostatni miałem widok przez okno w ścianie mojego pokoju, która pierwotnie była jedną z zewnętrznych. Okno to, niegdyś wychodzące na zewnątrz, teraz pozwalało zaglądać do środka.

Przez niemal wszystkie lata, które moja rodzina spędziła w domu w Elizabeth City, pokój ten należał do mnie, podobnie jak okno przysłonięte firaną prawie w ogóle niezapewniającą prywatności. Od kiedy pamiętam, moim ulubionym zajęciem było jej odsuwanie i zerkanie przez szybę na to, co się działo w salonie. Innymi słowy, odkąd pamiętam, moim ulubionym zajęciem było szpiegowanie.

Szpiegowałem moją starszą siostrę Jessikę. Jej pozwalano chodzić spać później ode mnie i oglądać kreskówki, na które byłem za mały. Szpiegowałem mamę Wendy, jak składała pranie, siedząc na kanapie i oglądając nocne wiadomości. Jednak osobą, którą podglądałem najczęściej, był mój tato Lon – czy raczej, jak to się mówi na

amerykańskim południu, Lonnie – okupujący salon do wczesnych godzin porannych.

Tato służył w Straży Wybrzeża, ale wtedy nie miałem najmniejszego pojęcia, co to znaczy. Wiedziałem tylko, że czasem nosił mundur, a czasem nie. Wychodził z domu wcześnie i wracał późno, nierzadko z jakimś nowym gadżetem – kalkulatorem naukowym Texas Instruments TI-30, stoperem Casio na smyczy albo głośnikiem do domowego zestawu stereo. Niektóre z tych rzeczy mi pokazywał, inne gdzieś chował. Na pewno domyślasz się, które interesowały mnie bardziej.

Urządzenie, które wywołało we mnie największą ciekawość, przybyło pewnego wieczora niedługo po tym, jak musiałem iść spać. Leżałem w łóżku i już zacząłem zasypiać, kiedy usłyszałem kroki taty w korytarzu. Wstałem, odsunąłem firanę i obserwowałem. Tato trzymał tajemnicze opakowanie zbliżone rozmiarami do pudełka na buty. Wyciągnął z niego beżowy obiekt o kształcie pustaka, z którego wystawały splątane kable przypominające macki jednego z potworów zamieszkujących głębiny morskie w moich koszmarach.

Powolnymi metodycznymi ruchami – wynikającymi po części ze zdyscyplinowanego inżynierskiego podejścia, a po części ze starań, by nie robić hałasu – tato rozplątał kable i poprowadził jeden z nich, wystający z tyłu urządzenia, w poprzek dywanu, do tylnego panelu telewizora. Następnie wpiął drugi kabel do gniazdka elektrycznego za kanapą.

Nagle ekran telewizora rozświetlił się, a wraz z nim twarz mojego taty. Zwykle spędzał wieczory na kanapie, otwierając kolejne puszki napoju Sun Drop i obserwując biegających po boisku. Tym razem jednak działo się coś innego. Potrzebowałem tylko chwili, by poczynić najbardziej niesamowite spostrzeżenie mojego całego, choć trzeba przyznać, że krótkiego życia: tato kontrolował to, co działo się na ekranie telewizora.

Stanąłem twarzą w twarz z Commodore 64 – jednym z pierwszych komputerów do użytku domowego.

Nie miałem oczywiście pojęcia, czym jest komputer, ani tym bardziej, czy to, do czego używał go tato, było pracą, czy zabawą. Widziałem, że się uśmiecha i chyba dobrze bawi, ale koncentrował się na tym, co działo się na ekranie, równie mocno, co na wszystkich technicznych zadaniach, które wykonywał w domu. Wiedziałem tylko jedno: cokolwiek robił, chciałem robić to samo.

Od tego dnia za każdym razem, gdy tato przychodził do salonu i wyciągał beżową cegłę, stawałem na łóżku, odsuwałem firankę i szpiegowałem jego przygody. Pewnej nocy na ekranie pojawiła się spadająca piłka, a u dołu pozioma kreska. Tato musiał poruszać kreską w lewo i prawo, żeby odbijać piłkę, a ta burzyła mur złożony z klocków o różnych kolorach (*Arkanoid*). Innej nocy siedział przed ekranem pełnym kolorowych klocków o różnych kształtach, które cały czas spadały. Gdy poruszały się w dół, tato obracał je i przesuwał tak, by tworzyły pełne rzędy, które natychmiast znikały (*Tetris*). Pewnego razu zupełnie nie mogłem pojąć, co robi tato: odpręża się czy robi coś do pracy? Bo kiedy zerknąłem przez okno, zobaczyłem, że lata.

Tato, który zawsze wprawiał mnie w zachwyt, wskazując palcem prawdziwe helikoptery z bazy powietrznej Straży Wybrzeża, kiedy przelatywały obok domu, pilotował własny helikopter – na moich oczach, w naszym salonie. Wystartował z tyciej bazy przyozdobionej maleńką, powiewającą na wietrze amerykańską flagą, wzniósł się w nocne niebo pełne mrugających gwiazd i natychmiast runął na ziemię. Wydał cichy jęk, który zamaskował mój własny, a gdy tylko uznałem, że już po zabawie, tato pojawił się z powrotem w małej bazie z miniaturową flagą i próbował wystartować jeszcze raz.

Gra zwała się *Choplifter!*, a wykrzyknik nie tylko stanowił część jej nazwy, ale również dobrze oddawał wrażenia z zabawy. *Choplifter!* był emocjonujący. Przyglądałem się, jak tato raz za razem wylatuje z naszego salonu na misje rozgrywające się nad płaską, przypominającą księżyc pustynią, podczas których strzela do wrogich odrzutowców i czołgów i unika ich ognia. Helikopter co chwilę lądował i wznosił się w powietrze, ponieważ tato usiłował ratować tłum migających ludzików, transportując go w bezpieczne miejsce. To było moje pierwsze wyobrażenie o tacie: był bohaterem.

Okrzyk radości, który dobiegł z kanapy, kiedy miniaturowy helikopter po raz pierwszy dotarł bez szwanku do bazy z pełnym ładunkiem ludzików, był odrobinę za głośny. Tato błyskawicznie odwrócił głowę w stronę okna, żeby sprawdzić, czy mnie nie obudził, i spojrzał mi prosto w oczy.

Rzuciłem się na łóżko, naciągnąłem na siebie kołdrę i leżałem absolutnie bez ruchu, wsłuchany w ciężkie kroki taty zbliżające się do mojego pokoju.

Zapukał w okno.

– Hej, młody, miałeś być w łóżku już dawno temu. Wciąż nie śpisz?

Wstrzymałem oddech. Nagle tato otworzył okno, sięgnął do pokoju, podniósł mnie razem z kołdrą i resztą pościeli i wciągnął do salonu. Stało się to tak szybko, że moje stopy nawet nie dotknęły dywanu.

Zanim się zorientowałem, siedziałem u taty na kolanach jako jego drugi pilot. Byłem za młody i zbyt podekscytowany, by zdać sobie sprawę, że joystick, który mi wręczył, nie był podłączony. Liczyło się dla mnie tylko to, że mogłem latać razem z nim.

02_Niewidzialna_ściana|

Elizabeth City to urocze, średnich rozmiarów miasto portowe ze stosunkowo dobrze zachowanym historycznym centrum. Podobnie jak większość miejscowości założonych we wczesnym okresie amerykańskiego osadnictwa, wyrosło nad wodą, w tym wypadku na brzegach rzeki Pasquotank, której angielska nazwa powstała w wyniku zniekształcenia słowa z języka algonkińskiego oznaczającego „miejsce, gdzie rozdwaja się nurt”. Pasquotank spływa z obszarów zatoki Chesapeake, przecina bagna na pograniczu Wirginii i Karoliny Północnej, po czym uchodzi do estuarium Albermarle Sound pospołu z Chowan, Perquimans i innymi rzekami. Za każdym razem, gdy zaczynam się zastanawiać, jak inaczej mogło potoczyć się moje życie, wracam myślami do tego zlewiska: nieważne, jaką trasą woda płynie ze źródła, ostatecznie dociera w to samo miejsce.

Moja rodzina od zawsze była związana z morzem, szczególnie po stronie mamy, która pochodzi w bezpośredniej linii od ojców pielgrzymów. Jej pierwszym przodkiem, który postawił stopę na amerykańskiej ziemi, był John Alden, bednarz statku Mayflower. John został mężem pasażerki Priscilli Mullins, której przypadł wątpliwy zaszczyt bycia jedyną na pokładzie samotną kobietą w wieku umożliwiającym zawarcie małżeństwa, a zatem jedyną potencjalną kandydatką do ślubu wśród całego pierwszego pokolenia mieszkańców kolonii Plymouth.

Do zbliżenia Johna i Priscilli w okolicach Dnia Dziękczynienia niemal nie doszło, a to za sprawą ingerencji komendanta Plymouth, Mylesa Standisha. Jego miłość do Priscilli, odrzucenie przez pannę jego zalotów

i jej późniejsze wyjście za mąż za Johna posłużyły za kanwę dzieła literackiego, które przewijało się przez całe moje dzieciństwo. Nosiło tytuł *The Courtship of Miles Standish* (Zaloty Mylesa Standisha), a jego autorem był Henry Wadsworth Longfellow (również potomek Aldena i Mullins):

> W pokoju słychać jeno młodzieńca śpieszne pióro,
> Kreśli skrzętnie list ważny, bo Mayflower już czeka,
> Gotów ruszyć nazajutrz lub dzień później, jak Bóg da!
> To zaś listy Aldena, a w nich pełno Priscilli,
> Pełno imienia i sławy purytańskiej dziewczyny Priscilli!

Córka Johna i Priscilli, Elizabeth, była pierwszym dzieckiem Pielgrzymów urodzonym w Nowej Anglii. Moja mama, również Elizabeth, wywodzi się od niej, jednak prawie wyłącznie w linii żeńskiej, dlatego nazwiska jej przodkiń zmieniały się praktycznie z pokolenia na pokolenie: Alden poślubiła Pabodiego, ich córka – Grinella, ich córka – Stephensa, a córka Stephensów – Jocelina. Wszyscy moi przodkowie-marynarze żeglowali wzdłuż wybrzeża, od terenów dzisiejszego Massachusetts po Connecticut i New Jersey – obsługując szlaki handlowe i unikając piratów grasujących pomiędzy koloniami a Morzem Karaibskim – aż z ustaniem wojny o niepodległość Ameryki ród Jocelinów osiedlił się w Karolinie Północnej.

Amaziah Jocelin, którego zapisywano też Amasiah Josselynem i na różne inne sposoby, był korsarzem i bohaterem wojennym. Przypisuje się mu, że jako kapitan wyposażonego w dziesięć dział barku The Firebrand bronił przylądka Fear w Karolinie Północnej. Po uzyskaniu niepodległości przez Stany Zjednoczone zamieszkał w mieście portowym Wilmington, gdzie objął stanowisko agenta, czyli oficera zaopatrzeniowego marynarki, i założył pierwszą miejską izbę handlową, którą nazwał, dość

humorystycznie, Intelligence-Office (Biuro Wywiadu). Jocelinowie i ich potomkowie – Moore’owie, Hallowie, Meylandowie, Howellowie, Stevensowie, Restonowie i Stokleyowie – którzy tworzą resztę drzewa genealogicznego mojej mamy, walczyli we wszystkich konfliktach zbrojnych w historii mojego kraju, od wojny o niepodległość i secesyjnej (w niej krewni z Karoliny bili się po stronie Konferedacji z kuzynami reprezentującymi Nową Anglię i Unię), po obie wojny światowe. Moja rodzina jest jedną z tych, które zawsze gotowe są służyć narodowi.

Ojciec mojej mamy – nazywam go zwyczajnie dziadkiem – to kontradmirał Edward J. Barrett. Kiedy się urodziłem, był zastępcą naczelnika działu inżynierii lotniczej Straży Wybrzeża w siedzibie głównej w Waszyngtonie. W swojej karierze obejmował najróżniejsze stanowiska dowódcze o charakterze inżynieryjnym i operacyjnym, od Governors Island w Nowym Jorku po Key West na Florydzie, gdzie był dyrektorem Połączonej Międzyagencyjnej Grupy Operacyjnej Wschód (formacji pod przywództwem amerykańskiej Straży Wybrzeża zrzeszającej wiele agencji z różnych krajów i mającej za cel zwalczanie przemytu narkotyków w basenie Morza Karaibskiego). Nie zdawałem sobie sprawy, jak wysoko w hierarchii piął się dziadek, ale zauważałem, że ceremonie towarzyszące obejmowaniu przez niego dowództwa stawały się coraz bardziej wyszukane – przemówienia były coraz dłuższe, a torty coraz większe. Przypominam sobie pamiątkę, którą wręczył mi pewien gwardzista artyleryjski podczas jednej z uroczystości: łuskę, wciąż gorącą, woniejącą prochowym piekłem, od pocisku kalibru 40 mm wystrzelonego przed chwilą na cześć dziadka.

Powinienem również wspomnieć o moim tacie Lonie, który w dniu moich narodzin był starszym bosmanem sztabowym w szeregach Straży Wybrzeża i pełnił służbę w Lotniczym Ośrodku Szkolenia Technicznego

w Elizabeth City, gdzie był projektantem planów nauczania i instruktorem elektroniki. Często wyjeżdżał na dłużej, zostawiając siostrę i mnie pod opieką mamy. Mama dbała, byśmy rozwijali w sobie poczucie odpowiedzialności – po to wyznaczała nam obowiązki. Nauczyła nas czytać w taki sposób, że do wszystkich szuflad w naszych komodach przyczepiła karteczki opisujące zawartość: SKARPETY, BIELIZNA. Ładowała nas do wózka Red Flyer i pchała go do miejscowej biblioteki, gdzie natychmiast ruszałem w stronę mojego ulubionego działu, który nazywałem „wielkie masini". Za każdym razem, gdy mama pytała, czy chciałbym poczytać o jakiejś konkretnej „wielkiej masinie", wpadałem w słowotok:

– O wywrotkach i o walcach drogowych, i o wózkach widłowych, i o żurawiach, i…

– To wszystko, synku?

– No nie… – odpowiadałem. – Jeszcze o betoniarkach, no i o buldożerach, i…

Mama uwielbiała dawać mi zadania matematyczne. Kiedy odwiedzaliśmy markety Kmart albo Winn-Dixie, mówiła, żebym wybrał sobie książki, modele samochodów osobowych oraz ciężarówek, i kupowała mi je, jeśli tylko udało mi się dodać w myślach ich ceny. Podnosiła poziom tego wyzwania wraz z moim wiekiem. Najpierw wystarczało, że zaokrąglę wynik do pełnego dolara, później musiałem podawać dokładną cenę w dolarach i centach, a od pewnego momentu mama żądała, żebym obliczył sumę i dodał do niej trzy procent. Tego ostatniego żądania ni w ząb nie rozumiałem, przy czym nie chodziło mi o arytmetykę, lecz o sens.

– Po co? – spytałem.

– To się nazywa podatek – wyjaśniła mi mama. – Za każdym razem, gdy coś kupujemy, musimy zapłacić trzy procent rządowi.

– A co on z nimi robi?

– Podobają ci się drogi? A mosty? – zapytała. – Rząd wydaje te pieniądze na ich utrzymanie. I na książki do biblioteki.

Jakiś czas później przestraszyłem się, że zawiodły mnie moje obiecujące umiejętności matematyczne, bo suma, którą miałem w myślach, nie zgadzała się z widniejącą na wyświetlaczu kasy. Mama jednak ponownie wyjaśniła, w czym rzecz.

– Podnieśli podatek od sprzedaży. Teraz musisz dodawać cztery procent.

– Czyli teraz biblioteka dostanie jeszcze więcej książek? – spytałem.

– Miejmy nadzieję – odpowiedziała mama.

Moja babcia mieszkała kilka przecznic od nas, naprzeciw zakładu paszowo-młynarskiego i potężnego drzewa orzesznika jadalnego. Odwiedzałem ją od czasu do czasu, po drodze zbierając z ziemi orzechy pekanowe do prowizorycznego koszyka w postaci rozciągniętej koszulki, i kładłem się na dywanie obok długich, niskich regałów z książkami. Zwykle wybierałem sobie do towarzystwa *Bajki Ezopa* oraz moją chyba ulubioną pozycję, *Mitologię* Bulfincha. Przewracałem strony jedna za drugą, pochłaniając opisy latających koni, zagmatwanych labiryntów i gorgon o wężowych włosach, które przemieniały śmiertelników w kamień, czasem tylko robiąc sobie przerwę na rozłupanie kilku orzechów. Byłem zachwycony Odyseuszem, całkiem podobali mi się również Zeus, Apollo, Hermes i Atena, ale bóstwem, do którego miałem największy szacunek, zdecydowanie był Hefajstos: nieurodziwy bóg ognia, wulkanów, kowali i drwali, bóg majsterkowiczów. Odczuwałem dumę z tego, że potrafię przeliterować jego greckie imię, i z wiedzy, że od imienia jego rzymskiego odpowiednika, Wulkana, nazwano planetę, z której pochodził Spock ze *Star Treka*. Od samego początku intrygowało mnie fundamentalne założenie grecko-rzymskiego panteonu. Na szczycie takiej czy innej góry

mieszkała ekipa bogów i bogiń, którzy spędzali swoją nieskończoną egzystencję, głównie walcząc między sobą i podglądając to, co działo się wśród ludzi. Od czasu do czasu, gdy dostrzegli coś, co ich intrygowało bądź niepokoiło, przybierali postać jagnięcia, łabędzia bądź lwa i zstępowali z Olimpu, by zbadać sytuację i interweniować. Zwykle próby narzucenia śmiertelnikom woli bóstw prowadziły do katastrofy – ktoś się topił, obrywał piorunem albo zostawał przemieniony w drzewo.

Pewnego razu wziąłem do rąk ilustrowaną edycję legend o Królu Arturze i jego rycerzach. Przeczytałem w niej o kolejnej legendarnej górze. Ta z kolei znajdowała się w Walii. To tam miał fortecę despotyczny gigant Rhitta Gawr, który nie chciał pogodzić się z faktem, że epoka jego dominacji dobiegła końca, a światem będą w przyszłości rządzić władcy wybierani spośród ludzi. Uważał bowiem ludzkość za karłowatą i słabą. Pełen determinacji, by utrzymać się u władzy, zszedł ze szczytu i zaczął podbijać królestwo za królestwem, gromiąc armie. Po pewnym czasie udało mu się pokonać i zabić wszystkich królów Walii i Szkocji, a z ich bród wyplótł sobie pelerynę, którą nosił jako swego rodzaju krwawe trofeum. Następnie postanowił rzucić wyzwanie najpotężniejszemu z królów Brytanii, Arturowi. Dał mu wybór: albo sam zgoli brodę i się podda, albo Rhitta pozbawi go głowy i zetnie jego brodę sam. Artur, rozwścieczony butą potwora, wyruszył w stronę jego górskiej fortecy. Król i gigant stanęli naprzeciw siebie na najwyższym szczycie i toczyli walkę przez wiele dni, aż obrażenia otrzymane przez Artura sprawiły, że nie mógł jej już kontynuować. W ostatniej chwili, gdy Rhitta Gawr chwycił go za włosy, by obciąć mu głowę, król zebrał resztki sił i zatopił legendarny miecz w oku giganta, a ten runął martwy na ziemię. Drużyna Artura zaczęła budować kamienny kopiec na zwłokach Rhitty, ale zanim skończyli, spadł śnieg. Gdy

odjeżdżała, widziała jak zbrukana krwią peleryna wypleciona z bród odzyskuje nieskalaną biel.

Góra, o której mowa w legendzie, nazywała się Snaw Dun, co, jak wyjaśniał przypis, w staroangielskim oznacza „śnieżne wzgórze”. Dziś Snaw Dun nosi nazwę Snowdon. To dawno wygasły wulkan wznoszący się na około 1085 metrów, co czyni z niego najwyższy szczyt Walii. Pamiętam ekscytację, gdy natknąłem się na moje nazwisko w tym kontekście, a archaiczny zapis „Snaw Dun” sprawił, że po raz pierwszy w życiu doznałem namacalnego wrażenia, że świat jest starszy ode mnie, nawet od moich rodziców. Powiązanie z bohaterskimi wyczynami Artura, Lancelota, Gawaina, Parsifala, Tristana i pozostałych Rycerzy Okrągłego Stołu było dla mnie źródłem dumy, przynajmniej do czasu, gdy dowiedziałem się, że wyczyny te nie miały charakteru historycznego, lecz legendarny.

Lata później, wspierany przez mamę, przetrząsałem bibliotekę z nadzieją, że uda mi się oddzielić fakty od mitów. Odkryłem, że kiedy władcy Szkocji starali się wzmocnić pretensje do tronu angielskiego, między innymi przemianowali szkocki zamek Stirling na Snowdon w hołdzie legendarnemu zwycięstwu Artura. Rzeczywistość, dowiedziałem się, prawie zawsze jest bardziej skomplikowana i mniej atrakcyjna, niż byśmy chcieli, ale i często okazuje się na swój dziwny sposób ciekawsza niż mity.

Kiedy odkrywałem prawdę o Arturze, miałem już od dłuższego czasu obsesję na temat opowieści nowego rodzaju, snutych w inny sposób. W Boże Narodzenie 1989 roku w naszym domu pojawiła się konsola Nintendo, zamknięte w obudowie w dwóch odcieniach szarości urządzenie, które zawładnęło moim życiem do tego stopnia, że zaniepokojona mama wprowadziła zasadę: żeby wypożyczyć nową grę, musiałem przeczytać książkę. Gry były drogie, a ja, jako że opanowałem już do perfekcji te,

które przyszły z konsolą – jeden kartridż mieszczący tytuły *Super Mario Bros.* i *Duck Hunt* – byłem żądny nowych wyzwań. Jedyny kłopot polegał na tym, że w wieku sześciu lat nie potrafiłem czytać równie szybko, co przechodzić gier. Nadszedł czas na kolejny popis początkującego hakera. Zacząłem przynosić z biblioteki książki coraz krótsze albo zawierające dużo obrazków. Czytałem ilustrowane encyklopedie wynalazków pełne dziwacznych szkiców welocypedów i sterowców, a także komiksy, które – z czego zdałem sobie sprawę dużo później – były skróconymi, przeznaczonymi dla dzieci wersjami dzieł Juliusza Verne'a i H.G. Wellsa.

To jednak NES – tandetna, ale genialna ośmiobitowa konsola Nintendo – był głównym źródłem mojej edukacji. Z *The Legend of Zelda* dowiedziałem się, że świat istnieje po to, by go eksplorować, *Mega Man* dał mi do zrozumienia, że od wrogów można się wiele nauczyć, zaś *Duck Hunt…* cóż, *Duck Hunt* pozwolił mi pojąć, że nawet kiedy ktoś śmieje się z twoich niepowodzeń, nie możesz strzelić mu w łeb. Najważniejszą, chyba zresztą do dziś, lekcję w moim życiu odebrałem jednak od *Super Mario Bros.* Piszę to zupełnie szczerze. Proszę, żebyś potraktował mnie poważnie. *Super Mario Bros.*, wersja 1.0, jest prawdopodobnie najgenialniejszą scrollowaną poziomo grą platformową wszech czasów. Na początku Mario stoi przy lewej krawędzi legendarnego ekranu powitalnego, a od rozpoczęcia gry może się poruszać tylko w jedną stronę: w prawo. To z tego kierunku na ekran wtaczają się nowe elementy scenerii i wrogowie. Mario musi przebrnąć przez osiem światów liczących po cztery poziomy – na ukończenie zadania ma ograniczony czas – by dotrzeć do złowrogiego Bowsera i uwolnić księżniczkę Toadstool. Przez wszystkie trzydzieści dwa poziomy Mario ma za plecami coś, co w slangu miłośników gier komputerowych nazywa się niewidzialną ścianą. Nie pozwala mu ona się cofać. Mario i Luigi mogą zatem tylko iść naprzód – podobnie jak ja i ty.

Życie biegnie w jednym kierunku – upływającego czasu – i nieważne, jak daleko uda się nam dobrnąć, niewidzialna ściana zawsze będzie tuż za naszymi plecami, odcinając nas od przeszłości i popychając do wyprawy w nieznane. Dzieciak dorastający w małym miasteczku w Karolinie Północnej w latach osiemdziesiątych XX wieku musi dowiedzieć się skądś o własnej śmiertelności. Czemu by nie od dwóch włoskich imigrantów, braci hydraulików o niezaspokojonym apetycie na pieczarki rosnące w kanałach?

Pewnego dnia mój przechodzony kartridż odmówił posłuszeństwa – nieważne, ile w niego dmuchałem, gra *Super Mario Bros.* nie chciała się załadować. Tak się wtedy robiło, a w każdym razie sądziliśmy, że tak trzeba: dmuchało się w złącze kartridża, żeby oczyścić je z kurzu, śmieci i psiej sierści zbierających się w środku. Tym razem jednak mimo dmuchania zarówno w kartridż, jak i w szczelinę konsoli, w którą się go wsuwało, ekran telewizora wyświetlał fale i plamy, co – mówiąc oględnie – zaniepokoiło mnie.

Z perspektywy czasu sądzę, że moje Nintendo prawdopodobnie miało uszkodzone jedno z połączeń pinów gniazda kartridża, ale w wieku siedmiu lat nie miałem pojęcia, czym są piny, zatem przepełniły mnie frustracja i rozpacz. Najgorsze było to, że tato dopiero co wyjechał w dwutygodniową delegację i nie mógł mi pomóc w naprawie. W odróżnieniu od świata Mario w moim nie istniały żadne sztuczki ani rury pozwalające zaginać czas, dzięki którym tygodnie mogłyby minąć szybciej, postanowiłem więc przywrócić konsolę do ładu samodzielnie. Wiedziałem, że jeśli mi się powiedzie, tato będzie pod wrażeniem. Udałem się więc do garażu po jego szarą metalową skrzynkę z narzędziami.

Doszedłem do wniosku, że jeśli mam odkryć, co się zepsuło, muszę rozkręcić konsolę. Zasadniczo kopiowałem czy też usiłowałem kopiować

czynności, które wykonywał tato, kiedy siadał przy kuchennym stole i naprawiał nasz magnetowid albo magnetofon – dwa elementy wyposażenia domu na moje oko najbardziej przypominające Nintendo. Mniej więcej godzinę wykręcałem moimi niezbornymi i bardzo małymi dłońmi śruby krzyżakowe przy pomocy płaskiego śrubokręta, ale ostatecznie powiodło mi się.

Z zewnątrz konsola miała nieciekawą szarą barwę, za to w jej wnętrzu znajdował się kolorowy gąszcz. Z zielonej jak trawa płytki drukowanej wychodziła tęcza przewodów, pomiędzy dało się dostrzec błyski srebra i złota. Dokręciłem kilka elementów, poluzowałem parę innych – tak na chybił trafił – i na każdy podmuchałem. Następnie wytarłem wszystko papierowym ręcznikiem, co spowodowało, że musiałem jeszcze raz podmuchać na płytkę drukowaną, by usunąć strzępki papieru z igieł, które – co dziś już wiem – były wspomnianymi wcześniej pinami.

Kiedy zakończyłem czyszczenie i naprawy, nadszedł czas na ponowne złożenie. Możliwe, że nasz biszkoptowy labrador Treasure połknął jedną z maleńkich śrubek albo po prostu zgubiła się we włosiu dywanu, ewentualnie pod kanapą. I chyba nie umieściłem wszystkich podzespołów w prawidłowych miejscach, bo ledwie mieściły się w szarej obudowie. Wieczko ciągle odskakiwało, więc docisnąłem elementy dłonią tak, jak się to robi z ubraniami w przepełnionej walizce niedającej się łatwo zamknąć. Po kilku próbach obudowa zatrzasnęła się, ale tylko po jednej stronie, bo druga się wybrzuszyła. Kiedy wcisnąłem ją na miejsce, uniosła się ta część, którą zamknąłem najpierw. Bawiłem się w te przepychanki przez pewien czas, po czym poddałem się i podłączyłem konsolę do prądu.

Wcisnąłem przycisk „power”… i nic. Wcisnąłem „reset”… też nic. Więcej przycisków na obudowie nie było. Przed moją naprawą sąsiadujące z przyciskami światełko jarzyło się czerwienią stopionego metalu, ale teraz

nawet ono nie dawało śladu życia. Konsola była zdeformowana i bezużyteczna, a mnie zalała fala poczucia winy i lęku.

Wiedziałem, że kiedy tato wróci z delegacji, nie będzie ze mnie dumny i wskoczy mi na głowę jak Goomba. Bałem się jednak nie tyle jego złości, co tego, że sprawię mu zawód. Współpracownicy mojego taty widzieli w nim doskonałego inżyniera elektronika, który specjalizował się w awionice. Dla mnie był szalonym naukowcem, który próbował samodzielnie naprawiać wszystkie domowe sprzęty – gniazdka elektryczne, zmywarki do naczyń, termy i klimatyzatory. Kiedy tylko mi pozwalał, pełniłem funkcję jego pomocnika, dzięki czemu dowiedziałem się, jaką fizyczną przyjemność może sprawiać zrobienie czegoś samodzielnie i jak intelektualnie stymulujące może być stosowanie podstaw mechaniki; poznałem też fundamentalne zasady elektroniki – różnicę pomiędzy napięciem a natężeniem, między mocą a oporem elektrycznym. Każde zadanie, którego się wspólnie podejmowaliśmy, kończyło się albo udaną naprawą, albo przekleństwami taty; w drugim wypadku ciskał niemożliwy do odratowania sprzęt do znajdującego się po drugiej stronie pokoju kartonowego pudła pełnego bezpowrotnie zepsutych rzeczy. Nigdy nie pomyślałem o nim źle z powodu tych niepowodzeń. Bardzo imponowało mi to, że w ogóle miał odwagę próbować.

Kiedy tato wrócił do domu i odkrył, co zrobiłem NES-owi, ku mojemu zdziwieniu wcale się nie zdenerwował. Nie był, rzecz jasna, zadowolony, ale podszedł do sprawy z wyrozumiałością. Wyjaśnił, że zrozumienie, dlaczego i w jaki sposób coś poszło źle, było dokładnie tak samo ważne, jak wiedza, który element się zepsuł: odkrycie źródła problemu pozwalało zapobiec powtórzeniu się awarii w przyszłości. Tato pokazał mi po kolei wszystkie podzespoły konsoli, wyjaśniając nie tylko, jak się nazywały, ale za co odpowiadały i w jaki sposób ich współdziałanie z pozostałymi

elementami gwarantowało poprawne funkcjonowanie urządzenia. Tylko dzięki analizie poszczególnych części mechanizmu można było określić, czy system został zaprojektowany w sposób pozwalający mu jak najwydajniej wykonywać jego zadanie. Jeśli tak było i po prostu nie działał poprawnie, należało go naprawić. Jeśli nie, należało zmodyfikować go tak, by stał się wydajniejszy. Było to, zdaniem mojego taty, jedyne słuszne podejście do naprawy sprzętu, które nie podlegało dyskusji i stanowiło fundamentalny obowiązek każdego, kto posługiwał się technologią.

Jak wszystkie lekcje, których udzielał mi tato, i tę charakteryzowała użyteczność znacznie wykraczająca poza bieżące zadanie. Przede wszystkim miała mi uświadomić znaczenie samodzielności, o czym – jak twierdził tato – Ameryka zapomniała jakiś czas temu, między jego a moim dzieciństwem. Nasz kraj stał się jednym z tych, gdzie koszt wymiany uszkodzonego urządzenia na nowszy model był w większości wypadków niższy niż zlecenie naprawy specjaliście, co z kolei najczęściej kosztowało mniej niż zdobycie części i wymyślenie, jak naprawić urządzenie własnymi rękami. Prawidłowość ta zasadniczo gwarantowała tyranię technologii, utrwalaną nie przez technologię jako taką, lecz przez ignorancję wszystkich użytkowników codziennie korzystających z niej bez zrozumienia. Odmawiając poznania rudymentarnych zasad obsługi i utrzymania sprzętu, na którym polegasz, biernie na tę tyranię przyzwalałeś i godziłeś się na następujące warunki: póki twój sprzęt pracuje, będziesz pracował i ty, a kiedy się zepsuje, pozostaniesz bezradny. Będziesz na łasce przedmiotów, które posiadasz.

Okazało się, że prawdopodobnie wyłamałem tylko jeden lut, ale musieliśmy odkryć który, i tato chciał posłużyć się w tym celu specjalnym sprzętem pomiarowym; miał do niego dostęp w swoim laboratorium w bazie Straży Wybrzeża. Podejrzewam, że mógł przywieźć go do domu,

ale z jakiegoś powodu zamiast tego zabrał mnie do pracy. Sądzę, że po prostu chciał pokazać mi swoją pracownię. Uznał, że byłem gotów.

Mylił się. Było to najbardziej imponujące miejsce, jakie w życiu widziałem. Przebijało nawet bibliotekę. A także sklep Radio Shack w centrum handlowym Lynnhaven. Najmocniej utkwiły mi w pamięci ekrany. Samo laboratorium było puste i słabo oświetlone; ściany wykończono standardowym połączeniem beżu i bieli, obecnym w większości rządowych budynków. Jeszcze zanim tato zapalił światło, zahipnotyzowała mnie pulsująca poświata elektrycznej zieleni. „Po co tu jest tyle telewizorów?” – taka była moja pierwsza myśl, po niej zaraz nadeszła kolejna: „I dlaczego wszystkie są nastawione na ten sam kanał?”. Tato wyjaśnił, że to, co widzę, to nie telewizory, lecz komputery, ale ja, choć słyszałem wcześniej to słowo, nie wiedziałem, co znaczy. Początkowo chyba założyłem, że komputerami były te ekrany – monitory.

Tato następnie pokazał mi je jeden po drugim, starając się wyjaśnić, do czego służą: ten przetwarzał sygnały radarowe, tamten przekazywał transmisje radiowe, jeszcze inny symulował systemy elektroniczne samolotów. Nie będę udawał, że zrozumiałem z tego wiele. Komputery te były bardziej zaawansowane od zdecydowanej większości wykorzystywanych w sektorze prywatnym i przerastały moje najśmielsze wyobrażenia. Co prawda ich procesory potrzebowały pięciu minut, by załadować system operacyjny, monitory wyświetlały tylko jeden kolor, a głośników, mogących odtwarzać efekty dźwiękowe i muzykę, nie było, ograniczenia te jednak wyłącznie dodawały im powagi.

Tato usadził mnie na krześle, a następnie podniósł siedzenie tak wysoko, że prawie sięgałem blatu i spoczywającej na nim prostokątnej bryły plastiku. Po raz pierwszy w życiu miałem przed sobą klawiaturę. Tato ani razu nie pozwolił mi pisać na swoim Commodore 64, a w czasie, który

rodzice pozwalali mi samemu spędzać przed ekranem, byłem ograniczony do konsol wideo wyposażonych w kontrolery służące do grania. Komputery w laboratorium były profesjonalnymi maszynami ogólnego przeznaczenia, nie urządzeniami rozrywkowymi, i nie wiedziałem, jak je zmusić do pracy. Nie widziałem nigdzie pada, joysticka ani pistoletu – jedynym interfejsem była ta plastikowa prostokątna płyta pokryta rzędami klawiszy z nadrukowanymi literami i cyframi. Co więcej, litery były ułożone w kolejności innej niż ta, której nauczono mnie w szkole. Pierwszą literą nie było A, tylko Q, po niej następowały W, E, R, T i Y. Przynajmniej cyfry były uporządkowane we właściwym szyku.

Tato wyjaśnił mi, że każdy klawisz – każda litera i każda cyfra – ma przypisane konkretne zadanie, i to samo dotyczy ich kombinacji. I podobnie jak w wypadku przycisków na padzie albo joysticku, kiedy poznało się odpowiednie kombinacje, można było zdziałać cuda. Aby zademonstrować mi, co ma na myśli, sięgnął nade mną do klawiatury, wpisał jakieś polecenie i wcisnął klawisz „enter”. Na ekranie pojawił się – jak się potem dowiedziałem – edytor tekstowy. Tato wziął karteczkę samoprzylepną i długopis, nabazgrał jakieś litery i cyfry, po czym kazał mi je dokładnie wpisać na klawiaturze, a sam poszedł naprawić nasze Nintendo.

Kiedy tylko zostawił mnie samego, zacząłem odtwarzać jego bazgroły na ekranie, szukając odpowiednich klawiszy palcami wskazującymi. Jako leworęczne dziecko nauczone posługiwania się prawą ręką z miejsca uznałem to za najbardziej naturalną metodę pisania, z jaką kiedykolwiek się zetknąłem.

```
10 INPUT "JAK MASZ NA IMIE?"; IMIE$
20 PRINT "CZESC, " + IMIE$ + "!"
```

Może ci się to wydawać łatwe, ale nie jesteś – jak ja wówczas – małym chłopcem o pulchnych, krótkich palcach, który nawet nie wiedział, co to są

cudzysłowy, nie mówiąc już nawet o tym, że w celu ich wpisania trzeba przytrzymać klawisz „shift”. W końcu, po bardzo wielu próbach i błędach, udało mi się wpisać cały tekst. Wcisnąłem „enter” i ułamek sekundy później komputer zapytał mnie: **JAK MASZ NA IMIE?**

Byłem zafascynowany. Na kartce taty nie było instrukcji, co mam robić dalej, więc zdecydowałem się odpowiedzieć i raz jeszcze wcisnąłem klawisz „enter”, z którym już zdążyłem się zaprzyjaźnić. I nagle na czarnym tle ekranu pojawiły się litery emanujące radioaktywną zieloną poświatą: **CZESC, EDDIE!**

Tak wyglądał mój pierwszy kontakt z programowaniem i technologią komputerową: nauczyłem się, że maszyny te robią to, co robią, ponieważ ktoś im to nakazuje – w bardzo szczególny, bardzo staranny sposób. I nie ma znaczenia, że ten ktoś ma siedem lat.

Niemal natychmiast pojąłem ograniczenia urządzeń przeznaczonych do gier. Nie dawały takiej swobody jak systemy komputerowe z prawdziwego zdarzenia. Nieważne, czy chodziło o Nintendo, Atari, czy Segę – wszystkie konsole zamykały cię w poziomach i światach, które można było przemierzać, a nawet pokonać piętrzące się w nich trudności, ale nie zmieniać. Naprawione Nintendo wróciło do salonu, gdzie grywaliśmy z tatą w *Mario Karta*, *Double Dragona* lub *Street Fightera* na dwie osoby. Na tym etapie we wszystkich tych grach radziłem sobie znacznie lepiej od taty – było to pierwsze zajęcie, w którym go przerosłem – ale od czasu do czasu dawałem mu wygrać. Nie chciałem, by sobie pomyślał, że nie jestem mu wdzięczny.

Nie mam naturalnego talentu do programowania i nigdy nie uważałem się za dobrego programistę. Na przestrzeni kolejnych dziesięciu lat stałem się jednak wystarczająco kompetentny, by móc stanowić zagrożenie. Do dziś uważam, że w kodowaniu jest coś magicznego: wpisujesz polecenia

w dziwnych językach, a procesor zamienia je w działanie urządzenia zrozumiałe dla każdego z nas. Fascynowała mnie myśl, że programista w pojedynkę może stworzyć coś uniwersalnego, coś nieograniczonego żadnymi prawami, zasadami ani przepisami poza tymi, które da się sprowadzić do prostej relacji przyczynowo-skutkowej. Pomiędzy kodem, jaki wprowadzałem, a wynikami zwracanymi przez komputer istniał doskonały związek logiczny. Kiedy wydawałem wadliwe komendy, otrzymywałem błędne wyniki. Gdy moje polecenia nie zawierały błędów, komputer generował równie bezbłędny rezultat. Nigdy wcześniej nie spotkałem się z niczym tak spójnym i sprawiedliwym, tak jednoznacznie bezstronnym. Komputer czekał w nieskończoność na moją komendę, ale przetwarzał ją, kiedy tylko wcisnąłem „enter”, bez zadawania zbędnych pytań. Żaden z moich nauczycieli nie był tak cierpliwy ani nie reagował tak szybko na moje potrzeby. Nigdzie indziej – na pewno nie w szkole i nie w domu – nie miałem tak silnego wrażenia, że panuję nad swoim życiem. Fakt, że perfekcyjnie napisany zestaw komend niezmiennie prowadził do perfekcyjnego wykonania tego samego ciągu operacji, z czasem stał się dla mnie – podobnie jak dla wielu technicznie uzdolnionych dzieci z pokolenia dorastającego na przełomie millenium – jedyną niezachwianą i niepodważalną prawdą.

03_Chłopak_z_Beltway|

Tuż przed moimi dziewiątymi urodzinami przeprowadziliśmy się z Karoliny Północnej do Marylandu. Ku mojemu zaskoczeniu okazało się, że moje nazwisko jest tu dobrze znane. Zamieszkaliśmy w hrabstwie Anne Arundel, gdzie słowo „Snowden” spotyka się praktycznie na każdym kroku; musiało jednak minąć trochę czasu, zanim dowiedziałem się, z czego to wynika.

Brytyjski major Richard Snowden przybył do Marylandu w roku 1658, licząc na to, że gwarancje wolności religijnej, jakich lord Baltimore udzielił katolikom i protestantom, obejmą także kwakrów. W 1674 roku do Richarda dołączył jego brat, John; zgodził się on opuścić angielskie hrabstwo Yorkshire i wyemigrować do Ameryki w zamian za skrócenie wyroku więzienia, jaki wydano na niego za głoszenie kwakierskich nauk. Kiedy w 1682 roku William Penn pożeglował na statku Welcome w górę rzeki Delaware, John Snowden był jednym z nielicznych Europejczyków, którzy powitali go u celu jego podróży.

Po wybuchu amerykańskiej rewolucji trzech wnuków Johna Snowdena zaciągnęło się do Armii Kontynentalnej. Ściągnęło to na nich potępienie odrzucającej przemoc społeczności kwakrów, ale młodzi Snowdenowie zdecydowali się posłuchać głosu sumienia, który nakazywał im odstąpić od pacyfistycznych ideałów i wziąć czynny udział w walce o niepodległość. William Snowden, jeden z wnuków Johna i mój przodek w linii prostej ze strony ojca, dosłużył się w amerykańskiej armii stopnia kapitana. Wzięty do niewoli podczas bitwy o Fort Washington w stanie Nowy Jork, zmarł

wkrótce potem w jednym z owianych złą sławą obozów jenieckich, jakie brytyjskie władze kolonialne urządziły w magazynach trzciny cukrowej na Manhattanie (podobno Brytyjczycy uśmiercali przetrzymywanych tam jeńców, dosypując im do pożywienia sproszkowane szkło). Syn Williama i jego żony Elizabeth z domu Moor, oddanej zauszniczki generała George'a Washingtona, miał na imię John. Był politykiem, historykiem i wydawcą jednej z pensylwańskich gazet. Jego potomkowie porzucili Pensylwanię i przenieśli się na południe, osiedlając się w tej samej okolicy, gdzie mieszkali ich krewni, czyli Snowdenowie z Marylandu.

W 1686 roku król Karol II podarował rodzinie Richarda Snowdena 800 hektarów porośniętej lasem ziemi, niemal w całości położonej na terenie marylandzkiego hrabstwa Anne Arundel. Snowdenowie założyli tam między innymi Patuxent Iron Works, jedną z największych w kolonialnej Ameryce hut żelaza oraz wytwórni kul armatnich i karabinowych, a także zarządzany przez wnuków Richarda majątek rolny z polami uprawnymi, pastwiskami i mleczarnią. Po zakończeniu służby w Maryland Line, słynącej z bohaterstwa formacji Armii Kontynentalnej, wnukowie Richarda Snowdena powrócili do rodzinnego majątku i – aby w pełni urzeczywistnić wolnościowe ideały, o które walczyli podczas wojny o niepodległość – wyzwolili swoich dwustu czarnych niewolników, kładąc tym samym kres wykorzystywaniu przez Snowdenów pracy niewolniczej na prawie sto lat przed wojną secesyjną.

Dawne posiadłości Snowdenów są dziś przedzielone na pół aleją Snowden River Parkway – ruchliwą, czteropasmową ulicą, wzdłuż której wyrosły modne sieciowe restauracje oraz salony samochodowe. Nieopodal przebiega Patuxent Freeway, czyli odcinek autostrady stanowej nr 32 prowadzący prosto do Fortu George'a G. Meade'a, drugiej pod względem wielkości bazy wojskowej w Stanach Zjednoczonych, a zarazem siedziby

Narodowej Agencji Bezpieczeństwa (NSA). Fort Meade także powstał na gruntach należących niegdyś do moich krewnych, którzy albo sprzedali tę ziemię (jak twierdzi część), albo zostali z niej wywłaszczeni przez amerykański rząd (jak utrzymują inni).

Początkowo nie miałem o tym wszystkim pojęcia. Moi rodzice zażartowali sobie, że władze stanu Maryland zmieniają nazwiska na tablicach ulicznych za każdym razem, gdy sprowadza się tam ktoś nowy. W przeciwieństwie do rodziców nie widziałem w tym nic śmiesznego; ich żart przyprawił mnie wręcz o gęsią skórkę. Z Elizabeth City do hrabstwa Anne Arundel nie jest wcale tak daleko – dzieli je tylko nieco ponad czterystukilometrowy odcinek autostrady międzystanowej I-95 – a mimo to po przeprowadzce poczułem się tak, jakbym wylądował na innej planecie. Zamiast porośniętych bujną zielenią brzegów rzeki otaczały mnie betonowe chodniki. W poprzedniej szkole miałem dobre wyniki w nauce i byłem lubiany przez rówieśników; w nowej stałem się obiektem ciągłych docinków. Nabijano się z moich okularów, z braku zainteresowania sportem, a zwłaszcza z mojego akcentu. Ponieważ w typowy dla mieszkańców Południa sposób przeciągałem samogłoski, nowi szkolni koledzy nazywali mnie debilem.

Stałem się tak przeczulony na punkcie mojego południowego akcentu, że w ogóle przestałem odzywać się w szkole. Ćwiczyłem samotnie w domu, dopóki nie zacząłem mówić „normalnie” – a przynajmniej dopóki nie nauczyłem się wymawiać lokalizacji moich upokorzeń jako *English class*, zamiast *Anglish clay-iss*, a słowa „palec” jako *finger* zamiast *fanger*. Zanim w końcu nabrałem odwagi, by ponownie zacząć odzywać się na lekcjach, moje oceny mocno się pogorszyły, a niektórzy nauczyciele postanowili poddać mnie testowi na inteligencję, bo nabrali podejrzeń, że cierpię na poważne trudności w nauce. Kiedy przyszły wyniki, nie przypominam

sobie, żebym doczekał się jakichkolwiek przeprosin – zamiast tego wysłano mnie na całą masę zajęć pozalekcyjnych, mających „wspierać rozwój zainteresowań”. Mało tego, ci sami nauczyciele, którzy wcześniej powątpiewali w moją zdolność przyswajania wiedzy, teraz zaczęli mieć jakiś problem z tym, że polubiłem zabierać głos na forum klasy.

Miejsce, dokąd trafiliśmy po przeprowadzce z Karoliny Północnej, zwane jest Beltway, czyli obwodnica. W przeszłości nazywano tak autostradę międzystanową nr 495 pełniącą funkcję obwodnicy Waszyngtonu, ale obecnie mianem Beltway określa się rozległy i wciąż rozrastający się pierścień sypialnianych miast, miasteczek i osiedli wokół amerykańskiej stolicy. Rozciąga się on od Baltimore w stanie Maryland na północy aż po Quantico w Wirginii na południu. Mieszkańcami tych stołecznych peryferii są niemal wyłącznie urzędnicy rozmaitych rządowych instytucji oraz pracownicy prywatnych firm, prowadzących interesy z rządem Stanów Zjednoczonych. Powiedzmy sobie szczerze: nikt inny nie ma powodu, by tam się sprowadzać.

Zamieszkaliśmy w Crofton w stanie Maryland, w połowie drogi między Annapolis a Waszyngtonem. Crofton leży na zachodnim krańcu hrabstwa Anne Arundel; w tamtejszej architekturze mieszkalnej dominują wariacje na temat stylu federalnego oraz elewacje wykończone panelami winylowymi. Osiedla takich domów noszą zazwyczaj fantazyjne, staroświecko brzmiące nazwy: Crofton Towne, Crofton Mews, The Preserve albo The Ridings. W samym centrum naszego starannie zaprojektowanego miasteczka znajdował się elegancki ośrodek rekreacyjno-wypoczynkowy Crofton Country Club. Kiedy spojrzy się na mapę, Crofton przywodzi na myśl ludzki mózg: ulice wiją się, przecinają i splatają ze sobą niczym bruzdy pomiędzy fałdami kory mózgowej. Dom, do którego się wprowadziliśmy, stał przy Knightsbridge Turn – szerokiej,

spokojnej uliczce w kształcie półkola; wzdłuż niej wznosiły się dwukondygnacyjne budynki z szerokimi podjazdami i podwójnymi garażami. Nasz dom był siódmy w kolejności, licząc od obu końców ulicy – znajdował się więc dokładnie pośrodku tego półkola. Miałem dziesięciobiegowy rower marki Huffy i pracę rozwoziciela gazet – dostarczałem okolicznym mieszkańcom egzemplarze tytułu „The Capital”. Dziwnym trafem dystrybucja tej szacownej wydawanej w Annapolis gazety zaczęła w tamtym czasie poważnie szwankować – problemy z dostarczaniem gazet nasilały się w okresie zimowym i występowały zwłaszcza na obszarze między Crofton Parkway a Defense Highway (taką nazwę nosi przecinający Crofton odcinek drogi stanowej nr 450).

Dla moich rodziców był to ekscytujący okres. Przeprowadzka do Crofton wiązała się dla nich z awansem zarówno finansowym, jak i społecznym. Wysadzane drzewami ulice były niemal wolne od przestępczości, a wielokulturowa, wielorasowa i wielojęzyczna społeczność miasteczka – odzwierciedlająca różnorodną populację całego Beltway, składającą się w znacznej mierze z pracowników korpusu dyplomatycznego i agencji wywiadowczych – była zamożna i dobrze wykształcona. Tuż za naszym domem rozciągało się pole golfowe, za rogiem znajdowały się korty tenisowe, a kawałek dalej mieścił się pełnowymiarowy basen olimpijski. Pod względem dojazdów do pracy życie w Crofton także było bliskie ideału. Mój ojciec, służący wówczas w Straży Wybrzeża w stopniu starszego chorążego, potrzebował zaledwie czterdziestu minut, by dojechać do nowej pracy w Instytucie Inżynierii Lotniczej w kwaterze głównej Straży Wybrzeża, która w tamtym czasie zlokalizowana była w Buzzards Point, w południowej dzielnicy Waszyngtonu, nieopodal bazy wojskowej w Forcie Lesleya J. McNaira. Z kolei moja mama już po dwudziestu minutach jazdy samochodem docierała do nowej pracy w siedzibie NSA,

której futurystyczne, pudełkowate gmachy zwieńczone kopułami radiolokatorów i pokryte warstwą miedzi, zabezpieczającą przed podsłuchami i przechwytywaniem sygnałów elektronicznych, znajdują się w samym sercu Fortu Meade.

Osobom z zewnątrz może się to wydać dziwne, dlatego muszę wyraźnie podkreślić: fakt, że oboje moi rodzice wykonywali takie prace, nie był w Crofton niczym nadzwyczajnym. Sąsiedzi mieszkający na lewo od nas byli zatrudnieni w Departamencie Obrony; na prawo od nas mieszkało z kolei małżeństwo urzędników Departamentu Energii oraz Departamentu Handlu. Był taki czas, że wszystkie moje szkolne koleżanki, w których się podkochiwałem, miały ojców z FBI. Fort Meade był dla mnie po prostu miejscem pracy mojej mamy. Oprócz niej pracowało tam jeszcze 125 tysięcy osób, mniej więcej 40 tysięcy z nich mieszkało na terenie bazy, nierzadko z całymi rodzinami. W Forcie Meade ma swoje siedziby 115 różnych agencji rządowych, a także jednostki wojskowe należące do wszystkich pięciu rodzajów sił zbrojnych Stanów Zjednoczonych. Hrabstwo Anne Arundel liczy sobie niewiele ponad pół miliona mieszkańców, z czego jedną osiemsetną stanowią pracownicy poczty; co trzydziesty mieszkaniec hrabstwa zatrudniony jest w szkolnictwie, za to aż co czwarty pracuje lub pełni służbę w agencjach rządowych, firmach i instytucjach powiązanych w ten czy inny sposób z Fortem Meade. Baza posiada własne urzędy pocztowe, szkoły, komisariaty policji i jednostki straży pożarnej. Mieszkające w okolicy dzieci, zarówno te z rodzin wojskowych, jak i cywilnych, każdego dnia tłumnie przybywają do bazy, żeby uczestniczyć w organizowanych tam zajęciach golfa, tenisa i pływania. Chociaż nasza rodzina miała dom poza bazą, moja mama regularnie kupowała w tamtejszych kantynach hurtowe ilości artykułów spożywczych. W wielobranżowym sklepie wojskowym PX, czyli Post

Exchange, zaopatrywała mnie i moją siostrę w praktyczne i – co najważniejsze – sprzedawane w cenach netto ubrania, z których błyskawicznie wyrastaliśmy. Czytelnicy, którzy nie wychowywali się w takim środowisku, mogą spróbować wyobrazić sobie Fort Meade i jego otoczenie, a może nawet cały obszar Beltway jako gigantyczne miasto, całkowicie uzależnione od jednego pracodawcy dającego zatrudnienie większości mieszkańców. Tutejsza monokultura ma sporo wspólnego z monokulturą produkcyjną Doliny Krzemowej – tyle tylko, że produktem wytwarzanym w Beltway jest nie technologia, lecz instytucje rządowe.

Powinienem też dodać, że moi rodzice posiadali certyfikaty dostępu do informacji niejawnych, przy czym moja mama przeszła dodatkowo pełne badanie wariograficzne będące elementem bardziej rygorystycznych procedur bezpieczeństwa, jakim nie podlegają nawet osoby służące w wojsku. Jest to o tyle zabawne, że mama miała tak mało wspólnego ze szpiegostwem, jak to tylko możliwe. Pracowała w towarzystwie ubezpieczeniowo-emerytalnym obsługującym pracowników NSA – można więc powiedzieć, że przygotowywała pracownicze plany emerytalne dla szpiegów. Mimo to, żeby móc zajmować się obsługą takich świadczeń, musiała najpierw zostać prześwietlona tak szczegółowo, jakby miała zostać zrzucona na spadochronie do dżungli i zorganizować zamach stanu.

Jeśli chodzi o szczegóły kariery zawodowej mojego taty, to do dziś mam o nich dość mgliste pojęcie. Moja ignorancja w tej kwestii nie jest wcale czymś nietypowym. W świecie, w którym dorastałem, dorośli nie rozmawiali o swojej pracy – nie tylko z dziećmi, ale nawet z sobą nawzajem. To prawda, że wielu z nich obowiązywała tajemnica służbowa, jednak według mnie właściwszym wyjaśnieniem takiego zachowania jest techniczny charakter ich pracy i nacisk rządowych zleceniodawców na kompartmentalizację – powierzanie każdemu specjaliście tylko

niewielkiego wycinka większego projektu. Ludzie zajmujący się zawodowo nowoczesnymi technologiami rzadko, o ile w ogóle, mają pojęcie o szerszych zastosowaniach i politycznych konsekwencjach przedsięwzięć, w których realizację są zaangażowani. W dodatku ich praca wymaga tak bardzo specjalistycznej wiedzy, że gdyby spróbowali opowiedzieć o niej przy grillu, to nikt by już ich nigdzie nie zaprosił – takie rzeczy po prostu nikogo nie obchodzą.

Patrząc z perspektywy czasu, być może właśnie dlatego znaleźliśmy się w takiej sytuacji.

04_Online|

Wkrótce po tym, jak zamieszkaliśmy w Crofton, mój tato przyniósł do domu nasz pierwszy komputer stacjonarny: Compaq Presario 425. Jego cena katalogowa wynosiła 1399 dolarów, ale ojciec kupił go ze specjalną zniżką dla wojskowych. Początkowo nowy nabytek – ku rozpaczy mamy – stanął na środku jadalnianego stołu, a ja nie odstępowałem go na krok. Już wcześniej niechętnie wychodziłem z domu, żeby pokopać piłkę, a teraz już sama myśl o tym wydawała mi się niedorzeczna. Na zewnątrz nie było nic ciekawszego niż to, co miały mi do zaoferowania cuda techniki ukryte wewnątrz tego szarego, niezgrabnego peceta: niewiarygodnie szybki jak na tamte czasy 25-megahercowy procesor Intel 486 oraz twardy dysk o niewyczerpanej pojemności 200 megabajtów. Do tego – tylko to sobie wyobraź! – nasz komputer wyposażony był w kolorowy monitor – ściślej: ośmiobitowy kolorowy monitor, mogący wyświetlać 256 kolorów. (Sprzęt, jakiego używasz obecnie, wyświetla najprawdopodobniej miliony kolorów).

Compaq i ja staliśmy się nierozłączni – gdy tylko pojawił się w naszym domu, poczułem się tak, jakbym za jednym zamachem zyskał brata i spotkał moją pierwszą miłość. Mniej więcej w tym samym czasie wkroczyłem w wiek, w którym zacząłem odkrywać własne ja i uświadamiać sobie, że mój świat może składać się z rozmaitych światów, a ja mogę funkcjonować równocześnie w wielu z nich. Ten proces odkrywania siebie był tak ekscytujący, że zdarzało mi się zaniedbywać, a nawet zupełnie ignorować bliskich i tracić zainteresowanie

dotychczasowym życiem. Krótko mówiąc, przechodziłem burzliwy okres dojrzewania. A ponieważ przebiegało ono w cieniu nowoczesnej techniki, wiele zachodzących wówczas zmian w moim życiu było do pewnego stopnia udziałem każdego użytkownika komputera oraz internetu.

Komputer tak bardzo zaprzątał moją uwagę, że rano nie słyszałem ponagleń rodziców, bym szykował się do szkoły. Wieczorami byłem głuchy na upomnienia, żebym umył ręce przed kolacją. Dopiero kiedy zniecierpliwieni przypominali mi, że komputer nie jest wyłącznie moją własnością i ma służyć wszystkim domownikom, niechętnie ustępowałem miejsca ojcu, mamie lub siostrze. Jeśli moi bliscy chcieli w spokoju skorzystać z peceta, musieli wypraszać mnie z pokoju, bo inaczej z markotną miną zaglądałem im przez ramię i udzielałem porad, o które mnie wcale nie prosili: siostrze piszącej jakieś opracowanie w edytorze tekstu próbowałem pokazywać makropolecenia i skróty klawiaturowe albo podpowiadałem rozliczającym podatki rodzicom, jak lepiej korzystać z arkusza kalkulacyjnego.

Chciałem, żeby jak najszybciej zrobili to, co mieli do zrobienia, i pozwolili mi wrócić do moich znacznie ważniejszych zajęć. Na przykład do grania w *Loom*. Gry wideo, w które mój ojciec grywał kiedyś na komputerze Commodore, były bardzo proste i polegały na odbijaniu pingpongowej piłeczki albo sterowaniu helikopterem. Na początku lat dziewięćdziesiątych Commodore był już jednak mocno przestarzały; technika komputerowa poszła do przodu i zaczęły się pojawiać gry bardziej złożone. Ich twórcy zdawali sobie sprawę, że niemal każdy użytkownik komputera był jednocześnie zapalonym czytelnikiem, oczekującym od interaktywnej rozrywki nie tylko emocji, ale także ciekawej historii. W prymitywnych grach z okresu mojego dzieciństwa przeznaczonych na konsole Nintendo lub Sega albo na komputery Atari fabuła nie odgrywała

większej roli; zadaniem gracza było na przykład uratowanie prezydenta Stanów Zjednoczonych przed wojownikami ninja (naprawdę!). Z czasem tego rodzaju produkcje zaczęły ustępować miejsca grom z rozbudowaną warstwą fabularną, często inspirowaną starymi opowieściami i legendami, w jakich zaczytywałem się na dywanie w domu babci.

Gra *Loom* opowiadała o społeczności zwanej Tkaczami. Starszyzna Tkaczy (jej członkowie nosili te same imiona, co greckie bóstwa losu: Kloto, Lachesis i Atropos) stworzyła krosno, za pomocą którego można było sprawować kontrolę nad światem, czy też, jak głosił scenariusz gry, „wpływać na przeznaczenie, tworząc subtelne sploty nici, z jakich utkana jest rzeczywistość”. Pewien chłopiec, który poznał sekretną moc krosna, został skazany na wygnanie, po czym świat pogrążył się w chaosie. Ostatecznie wszyscy bohaterowie tej historii doszli do wniosku, że stworzenie narzędzia do manipulowania przeznaczeniem nie było wcale takim dobrym pomysłem.

Rzecz jasna, fabuła *Loom* nie miała nic wspólnego z rzeczywistością. Ale przecież to była tylko gra.

Z drugiej strony mimo młodego wieku nie umknęło mi, że magiczne krosno było swego rodzaju alegorią komputera, na którym grałem w *Loom*. Splatane za pomocą krosna wielobarwne nitki kojarzyły mi się ze splotami kolorowych przewodów, ukrytymi w obudowie komputera, a pojedyncza szara nić, która w świecie gry dawała wgląd w przyszłość, przywodziła mi na myśl długi szary kabel telefoniczny, wystający z tylnej ścianki komputera i łączący urządzenie z całym światem. To tutaj zaczynała się dla mnie prawdziwa magia. Szary kabel, karta modemowa naszego Compaqa oraz telefon podłączony do linii telefonicznej – to było wszystko, czego potrzebowałem, żeby nawiązać połączenie i zyskać dostęp do nowego wynalazku zwanego internetem.

Ci spośród czytelników, którzy urodzili się w nowym tysiącleciu, mogą nie dostrzegać w dostępie do internetu niczego ekscytującego. Ale wierz mi – wtedy była to naprawdę niesamowita sprawa. W dzisiejszych czasach dostęp do sieci to coś oczywistego. Smartfon, laptop, komputer stacjonarny – każde z tych urządzeń jest dziś stale połączone. Z czym? I w jaki sposób? Takimi pytaniami nikt nie zawraca sobie głowy. Wystarczy, że stukniesz w ikonę przez twoich starszych krewnych nazywaną „przyciskiem internetu”, i gotowe: możecie przejrzeć najnowsze wiadomości, zamówić pizzę albo skorzystać ze strumieniowej transmisji danych, żeby posłuchać muzyki albo obejrzeć materiały filmowe, które kiedyś nazywaliśmy telewizją i kinem. Ale gdy miałem dwanaście lat, życie nie było takie proste: mieliśmy pod górkę do szkoły – i ze szkoły również – a żeby skorzystać z internetu, musieliśmy najpierw własnoręcznie podłączyć modem do gniazdka telefonicznego.

Nie twierdzę, że posiadałem wtedy jakąś rozległą wiedzę na temat tego, czym jest internet albo na czym dokładnie polega proces łączenia się z siecią, ale zdawałem sobie sprawę, że mam do czynienia z czymś fascynującym. W tamtych czasach po wydaniu komputerowi polecenia połączenia się z internetem urządzenie zaczynało rozbrzmiewać głośnymi trzaskami, piskami i syczeniem, zupełnie jakby w jego wnętrzu obudziło się kłębowisko węży – mogło to trwać całe wieki, a co najmniej kilka dobrych minut. Kiedy połączenie zostało wreszcie nawiązane, wystarczyło podnieść słuchawkę drugiego domowego telefonu podłączonego do tej samej linii i można było usłyszeć, jak komputery ze sobą rozmawiają. Naturalnie, nie dało się zrozumieć, co mówią, ponieważ porozumiewały się w języku maszyn, który umożliwiał przesyłanie czternastu tysięcy znaków na sekundę. Te niezrozumiałe dialogi stanowiły jednak dowód na to, że łącza

telefoniczne przestały służyć wyłącznie do pogaduszek prowadzonych przez nasze starsze, nastoletnie siostry.

Udostępnienie internetu masom i pojawienie się sieci World Wide Web było jak Wielki Wybuch albo eksplozja kambryjska naszych czasów. Nieodwracalnie odmieniło życie wszystkich ludzi, w tym moje. Mniej więcej od dwunastego roku życia starałem się spędzać każdą chwilę w sieci. Kiedy nie miałem takiej możliwości, zajmowałem się planowaniem następnej sesji online. Internet stał się moim azylem; zasoby sieci były moim placem zabaw, domkiem na drzewie, twierdzą, szkołą bez murów. Trudno to sobie wyobrazić, ale wychodziłem z domu jeszcze rzadziej niż wcześniej, a moja cera stała się jeszcze bladsza. Zarywane przed komputerem noce odsypiałem w szkole. Moje oceny ponownie poleciały na łeb na szyję.

Nie przejmowałem się jednak zbytnio problemami w szkole i nie jestem pewien, czy przejmowali się nimi moi rodzice. Wiedza, którą zdobywałem w internecie, wydawała się bardziej wartościowa i przydatna z punktu widzenia mojej przyszłej kariery niż cokolwiek, czego mogłem nauczyć się w szkole. A przynajmniej tak starałem się przedstawić to rodzicom.

Moja ciekawość nie miała granic, zupełnie jak internet, którego zasobów przybywało w tempie wykładniczym. Z każdym dniem, z każdą godziną, z każdą minutą powstawały nowe strony internetowe. Wiele z nich poświęconych było zagadnieniom, o których nie miałem większego pojęcia albo z których istnienia nie zdawałem sobie nawet sprawy. Ale gdy tylko natknąłem się na stronę poświęconą nieznanemu tematowi, natychmiast odczuwałem chęć zapoznania się z nim w najdrobniejszych szczegółach. Nieustannie chłonąłem nowe informacje, pozwalając sobie jedynie na krótkie przerwy na odpoczynek, szybką przekąskę albo wizytę w toalecie. Interesowały mnie nie tylko poważne kwestie techniczne w rodzaju porad,

jak naprawić zepsuty napęd CD-ROM. Sporo czasu spędzałem na stronach o grach komputerowych, szukając specjalnych kodów, które umożliwiały włączenie trybu nieśmiertelności w *Doomie* czy *Quake'*u. Byłem oszołomiony bezmiarem informacji dostępnym na wyciągnięcie ręki. Ledwo kończyłem zgłębiać jeden temat, a moją uwagę przykuwał już kolejny. Poradnik samodzielnego złożenia komputera potrafił rozbudzić moją ciekawość na tyle, że pogrążałem się w lekturze artykułu o architekturze procesorów. Dla odprężenia przeglądałem witryny o sztukach walki, broni palnej i sportowych samochodach, a także – skoro obowiązuje tu pełna jawność – strony z miękką i nieco twardszą pornografią w gotyckich klimatach.

Kiedy odzywał się we mnie głód wiedzy, czułem, że muszę dowiedzieć się wszystkiego na każdy interesujący mnie temat i nie spocznę, dopóki nie osiągnę tego celu. Moje próby nadążania za technologicznym postępem przypominały nieustający wyścig. W tym samym czasie większość nastoletnich chłopców ścigała się ze sobą w innych dyscyplinach: kto bardziej urośnie albo komu pierwszemu sypnie się na twarzy młodzieńczy zarost. W jeszcze innym wyścigu uczestniczyły te dzieciaki z mojej szkoły – byli wśród nich uczniowie z zagranicy – którym zależało na zyskaniu akceptacji rówieśników. Żeby tak się stało, musieli być *cool* i dlatego usilnie starali się nadążać za najnowszymi modami i trendami. Ale zdobycie nowego modelu bejsbolówki „No Fear" i wygięcie w odpowiedni sposób jej daszka wydawało mi się dziecinne – i zarazem dziecinnie proste – w porównaniu z moimi aspiracjami. Bycie na bieżąco ze wszystkimi informacjami, jakie pojawiały się na regularnie odwiedzanych przeze mnie witrynach i w poradnikach internetowych, stanowiło nie lada wyzwanie. Dodatkowe trudności pojawiały się, kiedy przynosiłem do domu wyjątkowo kiepską kartę ocen albo gdy nauczyciele zatrzymywali mnie za

karę po lekcjach – moi rodzice zakazywali mi wówczas korzystania wieczorem z komputera, jeśli następnego dnia musiałem iść do szkoły. Buntowałem się przeciw tym zakazom, bo nie mogłem znieść myśli, że kiedy jestem odcięty od internetu, w sieci pojawiają się coraz to nowe materiały, a ja nie mam do nich dostępu. W końcu po licznych rodzicielskich ostrzeżeniach zawisła nade mną groźba w postaci całkowitego szlabanu na korzystanie z komputera. Musiałem więc ustąpić. Zacząłem drukować na drukarce igłowej najciekawsze fragmenty tekstów znalezionych w sieci; wydruki zabierałem do łóżka i tam czytałem je wieczorami. Kiedy rodzice szli spać, ostrożnie uchylałem drzwi mojego pokoju i stąpając na palcach po skrzypiących schodach, przemykałem na parter, gdzie stał komputer. Ponieważ nie chciałem ryzykować włączania światła, musiałem zadowolić się nikłym blaskiem wygaszacza ekranu. Gdy już na wpół po omacku dotarłem do komputera, wybudzałem go z uśpienia i podłączałem do sieci – pamiętając o tym, by przycisnąć do jego obudowy poduszki i w ten sposób stłumić dźwięk tonowego wybierania numeru, a także szumy i syki, jakie wydawał z siebie modem podczas nawiązywania połączenia.

Jak wyjaśnić to wszystko komuś, kto tego nie przeżył? Moim młodszym czytelnikom, przyzwyczajonym do współczesnych standardów, może się wydawać, że raczkujący internet działał zdecydowanie za wolno, a pierwsze witryny były zbyt brzydkie i zbyt nudne, by w ogóle warto o nich wspominać. Ale to błędne przekonanie. W tamtych czasach bycie użytkownikiem internetu oznaczało prowadzenie równoległego życia, które większość internautów uznawała za diametralnie różne i całkowicie odrębne od życia w realu. Granica między rzeczywistością a światem wirtualnym nie uległa jeszcze wtedy zatarciu. I tylko od użytkownika zależało, gdzie ją wytyczy.

Ówczesny świat online był tak fascynujący, ponieważ pozwalał rozwinąć skrzydła wyobraźni i tworzyć od podstaw rzeczy zupełnie nowe. Web 1.0, czyli sieć pierwszej generacji, nie była wolna od wad – niektóre zastosowane w niej rozwiązania bywały nieintuicyjne i niepraktyczne – ale miała też zalety z nawiązką je rekompensujące. Zachęcała użytkowników do eksperymentowania i poszukiwania własnych form ekspresji, pomagając wyzwalać kreatywny potencjał jednostki. Wyobraźcie sobie typową witrynę internetową hostowaną na serwerach GeoCities: migające tło, które zmieniało kolor z zielonego na niebieski; biegnący przez środek strony biały pasek z przesuwającym się tekstem opatrzonym kilkoma wykrzyknikami – „Przeczytaj to koniecznie!!!” – a do tego animowany gif z tańczącym chomikiem. Wszystko to robiło wrażenie sporej nieporadności i trąciło amatorszczyzną, ale zarazem stanowiło dla mnie nieomylny znak, że mam do czynienia z niepowtarzalnymi wytworami ludzkiego intelektu i pomysłowości. Wykładowcy informatyki oraz inżynierowie systemowi, chałturzący po nocach absolwenci anglistyki oraz rezydujący w piwnicznych gabinetach samozwańczy specjaliści w dziedzinie ekonomii politycznej ochoczo dzielili się odkryciami i przemyśleniami. Robili to nie dlatego, że liczyli na finansowe profity; chcieli po prostu przekonać innych o słuszności swoich poglądów na taką czy inną kwestię. Śledziłem ich wywody z prawdziwym zainteresowaniem, niezależnie od tego, czy dotyczyły wyższości peceta nad makiem, zalet diety makrobiotycznej, czy też postulatu zniesienia kary śmierci. Entuzjazm internautów tej doby potrafił być naprawdę zaraźliwy. Wielu z tych dziwnych, a przy tym nierzadko błyskotliwych ludzi chętnie odpowiadało na moje pytania zadawane za pośrednictwem zamieszczonych na ich stronach formularzy kontaktowych („kliknij to hiperłącze albo skopiuj je i wklej do przeglądarki”) lub adresów e-mailowych (@usenix.org, @frontier.net).

Pod koniec XX wieku świat online zaczął ulegać postępującym centralizacji i konsolidacji. Instytucje rządowe i komercyjne coraz bardziej ingerowały w system, który na początku istnienia stanowił sieć równoprawnych użytkowników. Miałem to szczęście, że mój wiek dojrzewania przypadł niemal dokładnie na ów krótki, ale cudowny okres, kiedy to internet tworzyli ludzie dla ludzi i kiedy to ludzie byli jego najważniejszą częścią. Podstawową funkcją sieci nie było wówczas generowanie zysku, tylko dostarczanie informacji, a aktywność internautów regulowały nieustannie ewoluujący zbiór akceptowanych przez internetową społeczność zasad, a nie bezduszne i egzekwowalne prawnie umowy dotyczące warunków korzystania z usług. Do dziś uważam, że internet w latach dziewięćdziesiątych to najbardziej udana próba wprowadzenia w życie anarchistycznych ideałów.

W tamtych czasach byłem aktywnym użytkownikiem elektronicznych biuletynów informacyjnych, czyli tak zwanych BBS-ów (to skrót od angielskiej nazwy *bulletin-board system*). Po wybraniu nazwy użytkownika mogliście pisać i publikować dowolne wiadomości, dołączając do jednej z wcześniejszych dyskusji albo rozpoczynając nową. Wszystkie odpowiedzi na waszą wiadomość ukazywały się w formie wątku: wyobraźcie sobie najdłuższy łańcuch e-maili, z jakim mieliście do czynienia, tyle tylko, że dostępny dla każdego, kto chciał zapoznać się z przebiegiem debaty lub wziąć w niej udział. Oprócz BBS-ów istniały również specjalne programy do prowadzenia rozmów przez internet, takie jak Internet Relay Chat. Podobnie jak biuletyny sieciowe umożliwiały one komunikowanie się z innymi użytkownikami; różnica polegała na tym, że komunikacja odbywała się za pomocą wiadomości błyskawicznych. Dzięki temu można było prowadzić rozmowę na dowolny temat w czasie rzeczywistym, a przynajmniej w czasie możliwie zbliżonym do rzeczywistego, tak jak ma

to miejsce podczas rozmowy telefonicznej albo śledzenia emitowanej na żywo audycji radiowej czy telewizyjnej.

Większość wiadomości, jakie publikowałem w biuletynach sieciowych i wymieniałem za pośrednictwem klientów IRC, stanowiły pytania dotyczące składania mojego własnego komputera. Odpowiedzi, które otrzymywałem, były tak merytoryczne i szczegółowe, tak obszerne i uprzejme, że dziś wydaje się to nie do pomyślenia. Pewnego razu ogarnięty paniką usiłowałem się dowiedzieć, dlaczego chipset kupiony za pieniądze zaoszczędzone z kieszonkowego wydawał się niekompatybilny z płytą główną, którą dostałem w prezencie na gwiazdkę. Z pomocą pospieszył mi informatyk z drugiego końca kraju; napisał liczący dwa tysiące słów elaborat, wyjaśniając, na czym polega problem i jak mogę go rozwiązać. Nie ograniczył się do przepisania żywcem fragmentu jakiejś instrukcji – napisał swój tekst specjalnie z myślą o mnie i poprowadził mnie krok po kroku aż do rozwiązania mojego problemu. Miałem dwanaście lat, a mój internetowy rozmówca był dorosłym, zupełnie obcym człowiekiem, a jednak potraktował mnie po partnersku, ponieważ odnosiłem się do techniki z należnym szacunkiem. Ta życzliwość dla innych użytkowników, tak różna od agresywnego i złośliwego tonu, jaki dominuje w dzisiejszych mediach społecznościowych, wynikała moim zdaniem z wysokiego progu wejścia. W biuletynach sieciowych udzielali się wyłącznie pasjonaci, osoby mające odpowiednie umiejętności oraz stosowną dozę samozaparcia, ponieważ w latach dziewięćdziesiątych do korzystania z internetu nie wystarczało jedno kliknięcie. Samo zalogowanie się do sieci wymagało zadania sobie pewnego trudu.

Administratorzy jednego z moich ulubionych biuletynów sieciowych postanowili kiedyś zorganizować cykl towarzyskich spotkań stałych użytkowników; miały się odbywać w kilku różnych zakątkach kraju:

w Waszyngtonie, w Nowym Jorku, a także w Las Vegas, na targach elektroniki użytkowej Consumer Electronics Show. Presja na wzięcie udziału w tych zlotach była tak duża – organizatorzy roztaczali przed nami wizje szalonych wieczorów, wypełnionych jedzeniem i piciem – że ostatecznie nie miałem wyjścia i musiałem przyznać się publicznie do mojego wieku. Obawiałem się, że niektóre z korespondujących ze mną osób zaczną mnie ignorować, ale spotkałem się wyłącznie z przychylnymi reakcjami. Uczestnicy spotkania w Las Vegas zdali mi relację z odbywających się tam targów, a także wysłali mi zdjęcia oficjalnego katalogu; pewien gość zaoferował nawet, że prześle mi pocztą używane części komputerowe – zupełnie za darmo.

Może i wyjawiłem pozostałym użytkownikom BBS-ów, ile mam lat, ale nigdy nie zdradziłem, jak się nazywam. Jedną z największych zalet tych platform stanowił dla mnie fakt, że nie musiałem tam być sobą. Mogłem być kimkolwiek. Anonimowość czy też pseudonimowość BBS-ów zapewniała równowagę w relacjach pomiędzy użytkownikami, wyrównywała wszelkie dysproporcje. Mogłem ukryć się pod dowolnym pseudonimem, albo „nymem”, bo tak je czasem nazywano, i momentalnie stać się starszą, wyższą, dojrzalszą wersją samego siebie. Mogłem mieć nawet kilka różnych tożsamości jednocześnie. Korzystałem z nich, kiedy zadawałem pytania, które wydawały mi się bardziej dyletanckie, na forum tych biuletynów uznawanych przeze mnie za mniej fachowe – i za każdym razem robiłem to pod innym pseudonimem. Moje umiejętności i wiedza na temat komputerów rosły tak szybko, że zamiast być dumnym z poczynionych postępów, wstydziłem się mojej wcześniejszej ignorancji i chciałem się od niej odciąć. Chciałem oddzielić od siebie różne moje tożsamości. Powtarzałem sobie na przykład, jakim głupkiem musi być ten

squ33ker, który dawno temu – w zeszłą środę – zadawał pytania o kompatybilność swojego procesora.

Powiedzmy sobie jednak szczerze: pomimo etosu współpracy, kolektywizmu i wolnej kultury, jaki panował wśród ówczesnych pasjonatów internetu, współzawodnictwo między nimi bywało bezlitosne, a internetową społeczność – składającą się niemal w stu procentach z heteroseksualnych, buzujących hormonami mężczyzn – rozdzierały niekiedy błahe, ale niezwykle zażarte spory. Ponieważ jednak nikt nie występował pod prawdziwym nazwiskiem, osoby, które twierdziły, że was nienawidzą, nie były prawdziwymi ludźmi. Cała ich wiedza na wasz temat sprowadzała się do opinii, jaką wygłosiliście, oraz argumentów, jakimi się posłużyliście. Jeśli, albo raczej kiedy, jedna z waszych wypowiedzi wywołała wyjątkowe oburzenie pozostałych użytkowników, mogliście po prostu porzucić dotychczasowy pseudonim i przywdziać nową maskę. Pod jej osłoną mogliście nawet dołączyć do zbiorowego linczu na swojej dopiero co porzuconej tożsamości, zachowując się tak, jakbyście nie mieli z nią nic wspólnego. Nie potrafię opisać, jak wielka była to czasem ulga.

W latach dziewięćdziesiątych internet nie padł jeszcze ofiarą największej niegodziwości ery cyfrowej: podjęcia przez instytucje rządowe i komercyjne kroków w celu jak najściślejszego powiązania internetowych tożsamości użytkownika z jego tożsamością w świecie rzeczywistym. Każdy dzieciak mógł wejść do sieci i wypisać tam największe nawet głupoty, nie ryzykując przy tym, że nazajutrz zostanie obarczony odpowiedzialnością za to, co napisał. Ktoś mógłby powiedzieć, że nie jest to najzdrowsze środowisko do dorastania, ale moim zdaniem jest wprost przeciwnie – to jedyne środowisko, w którym młody człowiek może dorosnąć. Dzięki możliwości odcięcia się od naszych poprzednich sieciowych tożsamości, jaką początkowo oferował internet, osobom

z mojego pokolenia łatwiej było modyfikować przekonania i poglądy zamiast okopywać się na zajętych pozycjach i bronić ich za wszelką cenę w razie krytyki. Możliwość wymyślenia siebie od nowa oznaczała, że nie musieliśmy opowiadać się jednoznacznie po jednej stronie jakiegoś sporu ani popadać w bierność z obawy przed tym, że powiemy lub zrobimy coś, co nieodwracalnie zrujnuje naszą reputację. Błędy były błyskawicznie karane, ale też błyskawicznie korygowane, dzięki czemu zarówno winowajca, jak i cała społeczność mogli zapomnieć o danej sprawie i ruszyć naprzód. Dla mnie i dla wielu innych była to kwintesencja wolności.

Wyobraźcie sobie, że każdego dnia rano moglibyście przybierać nowe imię i nową twarz, jakie chcielibyście zaprezentować światu. Pomyślcie, że codziennie moglibyście wybierać sobie nowy głos i nowy sposób wysławiania się, tak jakby „przycisk internetu” był w istocie przyciskiem resetowania waszego życia. W nowym tysiącleciu technologia internetowa zaczęła służyć diametralnie innym celom: wymuszaniu wierności swojej historii, scalaniu tożsamości ze świata fizycznego i elektronicznego, a co za tym idzie, promowaniu ideologicznego konformizmu. Ale w latach dziewięćdziesiątych internet, przynajmniej przez chwilę, chronił nas, zapominając o naszych wykroczeniach i wybaczając nam grzechy.

Z mechanizmami internetowej autoprezentacji miałem do czynienia nie tylko na forum biuletynów sieciowych, ale przede wszystkim w znacznie bardziej fantastycznym środowisku: w pseudofeudalnych krainach i podziemiach, wykreowanych przez twórców gier fabularnych RPG (Role-Playing Game), a zwłaszcza MMORPG (Massively Multiplayer Online Role-Playing Game) – sieciowych gier fabularnych dla bardzo wielu graczy. Żeby zagrać w *Ultimę Online*, moją ulubioną grę z tego gatunku, musiałem stworzyć postać, a następnie wcielić się w moją alternatywną

tożsamość, tak zwany alt. W świecie gry mogłem być czarownikiem, wojownikiem albo złodziejem; mogłem też przełączać się między różnymi alternatywnymi tożsamościami z łatwością niewyobrażalną w świecie rzeczywistym, gdzie instytucje odnoszą się nieufnie do wszelkich prób zmiany tożsamości.

Przemierzałem wirtualne krainy *Ultimy* jako jeden z moich altów i wchodziłem w interakcje z altami innych graczy. Poznając je bliżej, na przykład podczas wspólnego wykonywania rozmaitych zadań, uświadamiałem sobie czasem, że zetknąłem się już wcześniej z danym graczem, który podczas naszego poprzedniego spotkania ukrywał się pod postacią innego alta. Pozostali mogli rozpoznać mnie w taki sam sposób. Czytali moje wiadomości i jeśli użyłem w nich charakterystycznego wyrażenia albo wysunąłem propozycję wykonania specyficznego zadania, mogli się zorientować, że chociaż w danej chwili wcielałem się w postać wojowniczki imieniem Shrike, to wcześniej byłem bardem Corwinem lub kowalem Belgarionem. Niekiedy takie spotkania były po prostu okazją do żartów i docinków, ale najczęściej traktowałem je jako okazję do rywalizacji – miarą sukcesu było dla mnie rozpoznanie większej liczby alternatywnych tożsamości drugiego gracza, niż on rozpoznał moich. Chcąc zdemaskować innych i jednocześnie pozostać pod przykrywką, musiałem przez cały czas zachowywać czujność i unikać powtarzania tych samych zwrotów w wysyłanych przeze mnie wiadomościach, a zarazem uważnie czytać komunikaty pisane przez innych graczy w nadziei, że nieopatrznie zdradzą prawdziwą tożsamość.

Alty zaludniające wirtualny świat *Ultimy* nosiły przeróżne imiona, ale ta pozorna różnorodność podlegała ograniczeniu przez klasy postaci, które były ściśle zdefiniowane, wręcz archetypiczne, i tak mocno osadzone w porządku społecznym świata gry, że odgrywanie konkretnej roli

przypominało niekiedy wypełnianie obywatelskiej powinności. Po całym dniu w szkole lub w pracy taki sposób spędzania wolnego czasu mógłby się wydawać pozbawiony sensu i nieprzynoszący satysfakcji, ale wcielając się wieczorem w rolę uzdrowiciela, pasterza, uczynnego alchemika lub maga mieliście poczucie, że robicie coś pożytecznego dla ogółu. Stosunkowa stabilność uniwersum *Ultimy* funkcjonującego według ustalonych praw i kodeksów postępowania sprawiała, że każdy alt miał specyficzne dla swojej roli społecznej zadania i był oceniany przez pryzmat swojej zdolności i gotowości do ich wypełniania.

Uwielbiałem tę grę i alternatywne życia, jakie mogłem dzięki niej przeżywać. Moja pasja sprawiała, że czułem się wolny, czego nie można jednak było powiedzieć o pozostałych członkach mojej rodziny. Gry komputerowe, a zwłaszcza sieciowe MMORPG, pochłaniają ogromne ilości czasu. Niezliczone godziny, jakie spędzałem na graniu w *Ultimę*, sprawiały, że nasze rachunki za telefon były niebotycznie wysokie, a w dodatku nie dało się do nas dodzwonić. Linia telefoniczna była nieustannie zajęta. Moja siostra, która wkroczyła w wiek późno nastoletni, kipiała z wściekłości na to, że moje przesiadywanie w internecie pozbawiało ją dostępu do najświeższych licealnych ploteczek. Dość szybko jednak wykoncypowała, że aby się na mnie zemścić, wystarczy podnieść słuchawkę telefonu, co powodowało zerwanie połączenia. Modem zamierał i zanim jeszcze moja siostra usłyszała w słuchawce sygnał wolnej linii, z parteru dobiegał mój rozpaczliwy krzyk.

Jeśli stracicie połączenie z siecią podczas czytania wiadomości na stronie internetowej, możecie po prostu połączyć się ponownie i wznowić lekturę w tym samym miejscu, w którym ją przerwaliście. Ale jeśli stracicie połączenie podczas rozgrywki w grę sieciową, w której nie można wcisnąć

pauzy ani zapisać jej stanu – ponieważ w tym samym czasie grają w nią tysiące innych użytkowników – to jesteście zgubieni. Mogliście być królem świata, legendarnym pogromcą smoków, posiadaczem własnego zamku i potężnej armii, ale wystarczyło, że minęło trzydzieści sekund od wyświetlenia się komunikatu POŁĄCZENIE PRZERWANE, by po ponownym zalogowaniu się do gry waszym oczom ukazywał się jasnoszary ekran z okrutnym epitafium: NIE ŻYJESZ.

Trochę mi dziś wstyd, kiedy pomyślę, jak poważnie wtedy do tego podchodziłem. Nie da się jednak ukryć, że wydawało mi się wówczas, że moja siostra celowo usiłuje zniszczyć mi życie – zwłaszcza wtedy, gdy wyzywająco spoglądała mi w oczy przed poniesieniem słuchawki telefonu na parterze. Robiła to nie dlatego, że musiała gdzieś zadzwonić, tylko po to, żeby mi przypomnieć, kto tu rządzi. W końcu nasi rodzice mieli już dość tych głośnych awantur i wykazali się zaskakującą wyrozumiałością. Zmienili abonament internetowy z naliczania opłaty za każdą minutę połączenia na stałą opłatę za nielimitowany dostęp do sieci i zainstalowali drugą linię telefoniczną.

Do naszego domu powrócił spokój.

05_Haker|

Każdy nastolatek jest hakerem. Musi nim być, ponieważ życie w tym wieku bywa trudne do zniesienia. Nastolatkowi wydaje się, że jest dorosły, podczas gdy dorośli uważają go za dziecko.

Spróbuj sięgnąć pamięcią do swoich nastoletnich lat. Też byłeś wtedy hakerem gotowym zrobić wszystko, byle tylko wyrwać się spod kurateli rodziców. Miałeś serdecznie dość, że traktują cię jak dzieciaka.

Przypomnij sobie, co czułeś, kiedy ktoś starszy i większy próbował tobą dyrygować, zupełnie jakby uważał, że skoro góruje nad tobą wiekiem i wzrostem, to siłą rzeczy także autorytetem. Twoim rodzicom, nauczycielom, ale także trenerom, drużynowym czy osobom duchownym z pewnością nie raz zdarzało się wykorzystywać uprzywilejowaną pozycję do tego, by wtrącać się w twoje prywatne sprawy, narzucać, jak ma wyglądać twoja przyszłość, i zmuszać do przestrzegania różnych anachronicznych zasad czy reguł. Dorośli, postrzegając nas przez pryzmat własnych marzeń, pragnień i nadziei, zawsze twierdzili, że robią to „dla naszego dobra” lub „w naszym najlepszym interesie”. I chociaż czasem była to prawda, to oczekiwaliśmy od nich czegoś więcej niż argumentu „bo ja tak mówię” bądź pustych zapewnień w rodzaju „kiedyś mi za to podziękujesz”. Każdy z nas nasłuchał się za młodu podobnych frazesów wygłaszanych z pozycji siły, co z góry wykluczało jakąkolwiek polemikę.

Dorastając, zaczynamy zdawać sobie sprawę, jak bardzo nasze życie podporządkowane jest zbiorom reguł, nieprecyzyjnych wytycznych i opresyjnych zasad, które stają się coraz bardziej nieznośne. Wymagania te

są nam narzucane i bywają zmieniane niemal bez uprzedzenia. Z istnienia niektórych nie zdajemy sobie nawet sprawy – aż do chwili, gdy nieświadomie zdarzy nam się je złamać.

Jeśli byłeś choć trochę podobny do mnie, to uświadomienie sobie tego wszystkiego musiało wywołać w tobie oburzenie.

Ja zaś byłem cierpiącym na krótkowzroczność chudzielcem, który ledwie co wkroczył w drugą dekadę życia, a już po raz pierwszy zaczął zadawać sobie pytania dotyczące polityki.

W szkole uczono nas, że w amerykańskim systemie politycznym obywatele delegują władzę przedstawicielom, których wybierają spośród siebie w wyborach powszechnych. Na tym polega demokracja. Ale demokratyczne reguły nie obowiązywały na lekcjach historii Stanów Zjednoczonych, ponieważ ani ja, ani moi koledzy nie mieliśmy tam prawa głosu – w przeciwnym wypadku nasz nauczyciel, pan Martin, szybko pożegnałby się z posadą. Zamiast tego pan Martin mógł samodzielnie ustalać zasady obowiązujące na jego lekcjach, tak jak pani Evans ustalała je wedle własnego widzimisię na zajęciach angielskiego, pan Sweeney – na lekcjach przyrody, a pan Stockton – na matematyce. Każdy z nauczycieli notorycznie zmieniał te reguły, zawsze z korzyścią dla siebie i zawsze po to, by jeszcze bardziej umocnić swoją władzę. Jeśli nie chciał wypuścić cię w trakcie lekcji do toalety, nie miałeś innego wyjścia, jak tylko zacisnąć zęby i wytrzymać do przerwy. Jeśli nauczyciel obiecał klasie wycieczkę do Instytutu Smithsońskiego, a następnie odwołał ją z powodu wykroczenia, jakiego rzekomo dopuścili się uczniowie, nie musiał uzasadniać decyzji – wystarczyło, że powołał się po prostu na własny autorytet i konieczność utrzymania dyscypliny. Szybko zrozumiałem, że wszelkie próby przeciwstawiania się regułom panującym w tym systemie są skazane na niepowodzenie, przede wszystkim dlatego, że każda zmiana zasad na takie,

które byłyby korzystniejsze dla większości uczestników, wymagałaby przekonania twórców owych zasad do dobrowolnego osłabienia swojej pozycji. Na tym właśnie polega podstawowy mankament czy też wada projektowa wprowadzana celowo do wszystkich systemów, zarówno politycznych, jak i informatycznych: ich twórcy nie mają powodów, by działać na własną niekorzyść.

O tym, że szkoła to system oparty na niesprawiedliwości, przekonał mnie fakt, że nie uznawał on żadnych uprawnionych form sprzeciwu. Mogłem bronić swoich racji aż do utraty głosu i niczego nie osiągnąć albo po prostu pogodzić się z tym, że żadne prawo głosu mi nie przysługuje.

Oświecona szkolna tyrania, tak jak wszystkie tyranie, nie jest systemem trwale stabilnym. Pozbawieni sprawczości nastoletni uczestnicy szkolnego systemu prędzej czy później decydują się stawić opór tyranii, przy czym – w sposób typowy dla osób w tym wieku – często mylnie utożsamiają opór z eskapizmem, a nawet z przemocą. Te dwie najbardziej popularne wśród nastolatków formy buntu w moim wypadku odpadały: miałem zbyt spokojne usposobienie, żeby dopuszczać się aktów wandalizmu, a zarazem nie byłem na tyle wyluzowany, by sięgać po narkotyki (do dziś ani razu nie zdarzyło mi się upić mocnym alkoholem; przez całe życie nie zapaliłem też ani jednego papierosa). Dlatego zająłem się hakowaniem – najrozsądniejszym, najbardziej pożytecznym i rozwijającym ze wszystkich znanych mi sposobów na zamanifestowanie przez nastolatka swojej niezależności i sprawienie, by dorośli zaczęli go traktować jak równego sobie.

Podobnie jak większość moich szkolnych kolegów nie lubiłem zasad, a jednocześnie nie miałem na tyle odwagi, by otwarcie je łamać. Dobrze wiedziałem, jak działa system. Wytykasz nauczycielowi błąd – dostajesz upomnienie. Naciskasz na belfra, który nie chce przyznać się do błędu – za

karę musisz zostać w szkole po lekcjach. Kolega ściąga od ciebie na sprawdzianie – czeka cię karna odsiadka po lekcjach, a kumpla – zawieszenie w prawach ucznia. Taka świadomość systemowych związków między wejściem a wyjściem, przyczyną a skutkiem, to fundament hakowania. Hakerstwo nie ogranicza się do systemów komputerowych; ma zastosowanie wszędzie tam, gdzie obowiązują jakieś zasady. Aby zhakować system, trzeba znać jego reguły lepiej niż ci, którzy go stworzyli albo nim zarządzają. Trzeba wykorzystać każdą rozbieżność pomiędzy tym, jak dany system miał działać, a tym, jak działa lub jak może działać w praktyce. Posługując się systemem w sposób niezamierzony przez jego twórców, haker nie tyle łamie jego reguły, co raczej obnaża ich słabości.

Natura zaprogramowała nas do rozpoznawania wzorców. Wszystkie decyzje podejmujemy na podstawie przechowywanych w pamięci założeń, zarówno empirycznych, jak i logicznych; nabywane nieświadomie założenia są następnie świadomie rozwijane. Na ich podstawie przewidujemy potencjalne konsekwencje zamierzonych przez nas działań; zdolność szybkiego i trafnego przewidywania następstw naszych wyborów w oparciu o posiadane informacje nazywamy inteligencją. Ale nawet najinteligentniejsi z nas polegają niekiedy na założeniach hipotetycznych, które nigdy nie zostały zweryfikowane – dlatego wszystkim nam zdarza się podejmować błędne decyzje. Ktoś, kto posiada większą od nas wiedzę albo potrafi szybciej i precyzyjniej rozumować, może wykorzystać nasze błędy do uzyskania rezultatów, jakich nigdy byśmy się nie spodziewali. Na tym polega egalitarny charakter hakerstwa – nie ma znaczenia, kim jesteś; liczy się wyłącznie twoja sprawność umysłowa. I to właśnie sprawia, że hakowanie jest niezwykle skutecznym narzędziem do rozprawy z zadufanymi w sobie autorytetami, tak głęboko przekonanymi

o bezbłędności swoich systemów, że przez myśl by im nie przeszło, by poddać je weryfikacji.

Rzecz jasna, nie dowiedziałem się tego wszystkiego w szkole. To internet pozwolił mi swobodnie zgłębiać interesujące mnie zagadnienia i odkrywać zachodzące między nimi zależności; dzięki niemu mogłem zdobywać wiedzę we własnym tempie, bez konieczności oglądania się na kolegów z klasy czy nauczycieli. Im więcej jednak czasu poświęcałem sieci, tym bardziej bezcelowe wydawało mi się spędzanie go w szkolnej ławce.

Latem, kiedy skończyłem trzynaście lat, postanowiłem, że nie wrócę już do szkoły, a przynajmniej mocno ograniczę zaangażowanie w wypełnianie szkolnych obowiązków. Problem polegał na tym, że nie bardzo wiedziałem, jak to zrobić. Każdy plan, jaki przychodził mi do głowy, narażał mnie na nieprzyjemne konsekwencje. Gdybym został przyłapany na wagarowaniu, rodzice ograniczyliby mi dostęp do komputera. Gdybym oświadczył, że postanowiłem rzucić szkołę, matka i ojciec z pewnością zakopaliby moje zwłoki głęboko w lesie, a potem opowiadaliby sąsiadom, że uciekłem z domu. Musiałem znaleźć jakieś inne rozwiązanie – i wpadłem na nie pierwszego dnia szkoły po wakacjach. A właściwie to zostało mi ono podane na tacy.

Każdy nauczyciel rozdał nam na pierwszej lekcji szczegółowo rozpisany program, jaki zamierzał z nami przerobić w semestrze, a także listę lektur obowiązkowych oraz terminarz klasówek, kartkówek i prac zaliczeniowych. Oprócz tego otrzymaliśmy zakres wymagań i kryteria oceniania, czyli informację o tym, w jaki sposób obliczane są poszczególne stopnie: A, B, C i D. Nigdy wcześniej nie miałem dostępu do takich informacji. Miałem wrażenie, że cyfry i litery układają się w równanie, którego wynik stanowi rozwiązanie mojego problemu.

Jeszcze tego samego dnia po powrocie do domu przeanalizowałem wszystkie sylabusy, starając się skalkulować, jakie wymagania z danego przedmiotu mogę zignorować i mimo to otrzymać zaliczenie. Weźmy na przykład historię Stanów Zjednoczonych. Według przygotowanej przez nauczyciela rozpiski na ocenę końcową z tego przedmiotu wpływały: stopnie z kartkówek (25 procent wszystkich możliwych do zdobycia punków), stopnie z klasówek (35 procent), prace semestralne (15 procent), prace domowe (15 procent) oraz najbardziej subiektywna kategoria, czyli aktywność na lekcjach (10 procent). Ponieważ z kartkówek i klasówek dostawałem na ogół dobre oceny, nie poświęcając przy tym zbyt wiele czasu na naukę, uznałem je za pewne źródło punktów potrzebnych do zaliczenia. Najbardziej czasochłonne były prace domowe i semestralne – miały niewielki wpływ na ocenę końcową, za to mocno ograniczały mój Czas Dla Siebie.

Obliczyłem, że gdybym zupełnie zaniechał odrabiania prac domowych, ale otrzymywał najwyższe oceny z pozostałych kategorii, to na koniec semestru miałbym na koncie 85 procent wszystkich możliwych do zdobycia punktów, co dawało ocenę B. Gdybym dodatkowo odpuścił pisanie prac semestralnych, uzbierałbym 70 procent punktów i otrzymałbym C z minusem. Pięć procent punktów za aktywność na lekcjach stanowiło mój margines bezpieczeństwa. Nawet gdyby nauczyciel przyznał mi w tej kategorii zero punktów – uznając moją aktywność za zakłócanie zajęć – to i tak miałbym na koncie 65 procent punktów, które przekładały się na ocenę D z minusem. To wystarczyło do otrzymania zaliczenia.

System opracowany przez naszych nauczycieli był z gruntu wadliwy. Informacje, które miały ułatwić uczniom zdobycie jak najwyższej oceny, mogły zostać wykorzystane do zdobycia jak największej wolności.

Stanowiły podpowiedź, jak uniknąć robienia tego, na co nie miałem ochoty, i jak mimo to zaliczyć dany przedmiot.

Gdy tylko na to wpadłem, przestałem zawracać sobie głowę pracami domowymi. Odtąd każdy kolejny dzień był czasem błogosławionej beztroski; beztroski niedostępnej tym, którzy muszą pracować i płacić podatki. I tak było aż do momentu, kiedy nauczyciel matematyki, pan Stockton, zadał mi na lekcji pytanie, dlaczego nie otrzymał ode mnie żadnego z sześciu zadań domowych. Brakowało mi wówczas sprytu, jaki przychodzi z wiekiem – zapomniałem, że ujawniając odkrytą w systemie lukę, pozbawiam się zdobytej przewagi. Ochoczo wyjaśniłem panu Stocktonowi, na czym polegały moje kalkulacje. Koleżanki i koledzy z klasy najpierw ryknęli śmiechem, a potem zaczęli skrobać coś w zeszytach, sprawdzając, czy oni także mogą sobie pozwolić na życie bez prac domowych.

– Spryciarz z ciebie, Eddie – stwierdził z uśmiechem pan Stockton, po czym przystąpił do omawiania tematu lekcji.

Przez mniej więcej dwadzieścia cztery godziny cieszyłem się sławą najbardziej łebskiego dzieciaka w całej szkole. Nazajutrz pan Stockton rozdał nam jednak nowe sylabusy. Widniała w nich informacja, że każdy uczeń, który do końca semestru nie odrobi więcej niż sześciu zadań domowych, automatycznie otrzyma ocenę niedostateczną.

Spryciarz z pana, panie Stockton.

Po lekcji nauczyciel przywołał mnie do siebie.

– Powinieneś wykorzystać swoje zdolności do tego, żeby jak najlepiej wykonywać pracę, a nie do tego, by jej unikać – powiedział. – Masz potencjał, Ed. Ale najwyraźniej nie zdajesz sobie sprawy, że oceny, które teraz otrzymujesz, zaważą na całym twoim życiu. Musisz zacząć myśleć o tym, co zostanie w twoich papierach.

Uwolniwszy się, przynajmniej chwilowo, od kieratu zadań domowych, miałem do dyspozycji więcej wolnego czasu. Wykorzystałem go na poznawanie bardziej konwencjonalnych sposobów hakowania, czyli takich, które wymagały użycia komputera. Moje umiejętności w tej dziedzinie zaczęły wkrótce rosnąć. Przesiadywałem w księgarniach i wertowałem odbite na kserokopiarce, spięte zszywkami strony hakerskich zinów, takich jak *2600* czy *Phrack*. Poznawałem opisane w nich techniki, a przy okazji przesiąkałem antyautorytarnym przesłaniem tych pism.

Znajdowałem się wówczas na samym dole technologicznej hierarchii; byłem nieopierzonym n00bem posługującym się narzędziami, których zasady działania wykraczały daleko poza moją wiedzę. Wiele osób wciąż zadaje mi pytanie, dlaczego – kiedy już nabrałem pewnej hakerskiej biegłości – nie zająłem się plądrowaniem kont bankowych albo wykradaniem numerów kart kredytowych. Prawda jest taka, że byłem zbyt młody i naiwny, by zdawać sobie sprawę, że coś takiego w ogóle było możliwe – nie mówiąc już o tym, że nie miałbym pojęcia, co zrobić z ukradzioną forsą. Wszystko, na czym mi zależało, wszystko, czego potrzebowałem, było dostępne zupełnie za darmo. Zamiast dokonywać zuchwałych kradzieży, wymyślałem proste sposoby na hakowanie gier komputerowych, przyznając sobie dodatkowe życia i zdolności takie jak widzenie przez ściany. Poza tym w tamtych czasach w internecie nie było zbyt wiele pieniędzy, przynajmniej jak na obecne standardy. Ze wszystkich hakerskich technik, o jakich wtedy słyszałem lub czytałem, najbliższy kradzieży był phreaking, czyli łamanie zabezpieczeń sieci telefonicznych umożliwiające wykonywanie darmowych połączeń.

Gdybyście zapytali któregoś z czołowych ówczesnych hakerów, dlaczego włamał się na stronę internetową jednego z największych serwisów informacyjnych tylko po to, żeby zastąpić jakiś nagłówek gifem

sławiącym umiejętności Barona von Hackerface'a – zresztą usuniętym zaledwie pół godziny później – usłyszelibyście odpowiedź podobną do tej, jakiej pewien słynny himalaista udzielił na pytanie, dlaczego wspina się na Mount Everest: „Bo istnieje". Większość hakerów, zwłaszcza tych młodszych, nie szukała w internecie władzy ani pieniędzy, tylko granic własnych umiejętności i okazji do udowodnienia, że nie ma rzeczy niemożliwych.

Byłem młody i kierowała mną czysta ciekawość, ale patrząc na to wszystko z perspektywy czasu, widzę wyraźnie, że niektóre z moich najwcześniejszych hakerskich prób podyktowane były także chęcią uśmierzenia trapiących mnie neurotycznych lęków. Im więcej dowiadywałem się o słabościach zabezpieczeń systemów komputerowych, tym bardziej obawiałem się konsekwencji zaufania nieodpowiedniej maszynie. Mój pierwszy nastoletni wyczyn hakerski, który wywołał pewne zamieszanie, związany był z prześladującą mnie wówczas obawą przed nuklearną zagładą, mogącą spustoszyć cały świat.

Po przeczytaniu pewnego artykułu poświęconego historii amerykańskiego programu jądrowego zacząłem szukać dalszych informacji na ten temat i zanim się obejrzałem, znalazłem się na stronie internetowej ośrodka badań jądrowych Los Alamos National Laboratory. Tak działa internet: coś wzbudza zainteresowanie i twoje palce przejmują kontrolę, prowadząc cię na coraz to nowe strony. Chwilę później struchlałem z przerażenia, bo odkryłem, że strona jednego z największych i najważniejszych w Ameryce ośrodków zajmujących się badaniami naukowymi i rozwojem broni, ma rażącą lukę w zabezpieczeniach. Był to wirtualny odpowiednik niezamkniętych drzwi: otwarta struktura katalogów.

Już wyjaśniam. Wyobraź sobie, że wysyłam ci link umożliwiający pobranie pliku PDF znajdującego się na osobnej podstronie

wielostronicowej witryny internetowej. Typowy adres URL takiego pliku mógłby wyglądać następująco: **strona.com/pliki/pdfy/nazwapliku.pdf**. Ponieważ struktura adresu URL odzwierciedla strukturę katalogów na serwerze, każda część adresu odpowiada odrębnej gałęzi drzewa katalogów. W omawianym przypadku w katalogu **strona.com** znajduje się folder **pliki**, zawierający podfolder **pdfy**, w nim zaś znajduje się plik **nazwapliku.pdf**, który zamierzasz pobrać. Obecnie większość witryn daje nam dostęp wyłącznie do podstrony z danym plikiem, nie ujawniając struktury katalogów. Ale w zamierzchłych czasach nawet największe witryny internetowe były tworzone i zarządzane przez ludzi, którzy stawiali dopiero pierwsze kroki w tej branży i często pozostawiali strukturę katalogów szeroko otwartą. W rezultacie wystarczyło skrócić rozbudowany adres URL pliku – w naszym przypadku zmienić go na przykład na **strona.com/pliki** – i uzyskiwało się dostęp do wszystkich plików na danej stronie, łącznie z tymi nieprzeznaczonymi dla postronnych użytkowników. Dokładnie tak przedstawiała się sytuacja w przypadku witryny ośrodka Los Alamos.

W społeczności hakerskiej tego rodzaju metoda uzyskiwania dostępu do zasobów strony uchodzi za odpowiednik raczkowania u niemowląt – jest to zupełnie podstawowa procedura, określana jako *dirwalking* lub *directory walking*, czyli spacer po katalogach. I to właśnie zrobiłem. Przechodziłem pospiesznie od plików do podfolderów, od podfolderów do folderów wyższego rzędu i z powrotem – nastolatek buszujący w katalogach. W ciągu pół godziny od przeczytania artykułu o zagrożeniach związanych z bronią jądrową odkryłem całą masę plików, do których dostęp powinni mieć wyłącznie pracownicy ośrodka jądrowego, posiadający odpowiednie poświadczenia bezpieczeństwa.

Nie ulega wątpliwości, że dokumenty, do których dotarłem, nie są żadnymi ściśle tajnymi planami i nie mógłbym w oparciu o nie skonstruować bomby atomowej we własnym garażu (poza tym tego rodzaju pliki z instruktażami i tak były już dostępne na co najmniej kilkunastu stronach „zrób to sam"). Większość dokumentów na stronie Los Alamos National Laboratory stanowiły rozmaite poufne notatki służbowe oraz dane osobowe pracowników ośrodka. Ponieważ jednak naprawdę obawiałem się grzybów atomowych na horyzoncie i, będąc dzieckiem rodziców pracujących w sektorze wojskowym, postanowiłem zrobić to, co wydawało mi się słuszne: poinformować o wszystkim dorosłych. Wysłałem do webmastera z Los Alamos e-mail z opisem odkrytej przeze mnie luki w zabezpieczeniach i czekałem na odpowiedź; ta jednak nigdy nie nadeszła.

Codziennie po szkole wchodziłem na stronę ośrodka, żeby sprawdzić, czy struktura katalogów uległa zmianie – nic się jednak nie zmieniało, z wyjątkiem mojego rosnącego zdumienia i oburzenia. W końcu sięgnąłem po telefon i zadzwoniłem pod podany na dole strony numer infolinii ośrodka.

Gdy tylko w słuchawce rozległ się głos pracownicy infolinii, momentalnie zacząłem się jąkać. Nie zdążyłem chyba nawet wydukać „struktura katalogów", gdy załamał mi się głos. Kobieta przerwała mi szorstkim „proszę czekać, łączę z działem informatycznym" i zanim zdążyłem jej podziękować, usłyszałem komunikat automatycznej sekretarki.

Udało mi się jakoś odzyskać odrobinę pewności siebie i opanowawszy nieco drżenie głosu, nagrałem wiadomość. Pamiętam jedynie uczucie ulgi, jakie mnie ogarnęło, kiedy już skończyłem. Na wszelki wypadek podałem raz jeszcze moje imię i nazwisko oraz numer telefonu. Wydaje mi się, że nazwisko przeliterowałem, posługując się wojskowym alfabetem

fonetycznym, jakiego używał niekiedy mój ojciec: „Sierra November Oscar Whiskey Delta Echo November”. Potem odłożyłem słuchawkę i wróciłem do swojego życia, które przez następny tydzień sprowadzało się właściwie wyłącznie do odwiedzania strony Los Alamos.

W dzisiejszych czasach, przy obecnych możliwościach rządowych agencji bezpieczeństwa cybernetycznego, każda osoba, która kilkadziesiąt razy dziennie łączyłaby się z serwerami Los Alamos National Laboratory, niemal na pewno stałaby się obiektem zainteresowania odpowiednich służb. Wtedy było jednak inaczej. Nie mogłem zrozumieć, jak to możliwe – czyżby moje zgłoszenie nikogo nie obchodziło?

Miały kolejne tygodnie – tak jak każdemu nastolatkowi, dłużyły mi się niczym miesiące – aż wreszcie któregoś dnia wieczorem, tuż przed kolacją, zadzwonił telefon. Odebrała moja mama, która przygotowywała w kuchni posiłek.

Ja siedziałem w tym czasie przed komputerem w jadalni. Dobiegające z kuchni strzępki rozmowy świadczyły o tym, że ktoś dzwonił do mnie: „Tak, mhm, jest tutaj”. A po krótkiej przerwie: „Mogę zapytać, kto mówi?”.

Odwróciłem się na krześle – mama stała nade mną, przyciskając słuchawkę do piersi. Była blada jak ściana. Drżała na całym ciele.

Zbolałym i pełnym niepokoju głosem, jakiego nigdy wcześniej nie słyszałem i który napędził mi niezłego stracha, wyszeptała:

– Coś ty narobił?

Gdybym wiedział, powiedziałbym jej. Zamiast tego spytałem tylko:

– Kto dzwoni?

– Los Alamos, laboratorium jądrowe.

– O, dzięki Bogu.

Delikatnie wyjąłem z ręki mamy telefon i posadziłem ją na krześle.

– Halo?

Dzwonił sympatyczny pracownik działu informatycznego z Los Alamos, zwracał się do mnie per „panie Snowden”. Podziękował mi za zgłoszenie problemu i poinformował, że już mu zaradzono. Powstrzymałem się przed zadaniem mu pytania, dlaczego trwało to tak długo – oraz przed sięgnięciem do komputera i sprawdzeniem, czy luka faktycznie została załatana.

Mama ani przez moment nie odrywała ode mnie wzroku. Próbowała poskładać w całość urywki rozmowy, ale słyszała tylko jedną stronę. Uniosłem do góry kciuk, żeby dać jej znać, że wszystko jest w porządku. Żeby ją o tym upewnić, przybrałem dojrzalszy, poważny i nieprzekonująco głęboki ton głosu i opowiedziałem informatykowi to, co już i tak wiedział: jak znalazłem lukę, jak ją zgłosiłem i jak przez długi czas na próżno czekałem na odpowiedź. Na koniec dodałem:

– Dziękuję, że zechciał pan zadzwonić. Mam nadzieję, że nie przysporzyłem państwu kłopotów.

– Ależ skąd – zapewnił informatyk, po czym zapytał, gdzie pracuję.

– Właściwie to nigdzie – odparłem.

Kiedy zapytał, czy nie szukam pracy, odpowiedziałem:

– W trakcie roku szkolnego jestem dość zajęty, choć mam sporo wolnych dni i wolne całe lato.

Dopiero wtedy zaskoczył, że ma do czynienia z nastolatkiem.

– W porządku, młody – powiedział. – Masz namiary na mnie. Odezwij się koniecznie, kiedy skończysz osiemnaście lat. A teraz daj mi jeszcze tę miłą panią, z którą wcześniej rozmawiałem.

Wręczyłem słuchawkę zatroskanej mamie. Wyszła z nią do kuchni, która zdążyła wypełnić się dymem. Kolacja się spaliła, ale informatyk z Los Alamos musiał powiedzieć mamie kilka pochlebnych rzeczy na mój temat, bo o żadnej karze – choć się jej spodziewałem – nie było mowy.

06_Zaległości|

Słabo pamiętam liceum, bo ogromną jego część przespałem, usiłując zrekompensować sobie bezsenne noce spędzone przed komputerem. Większości nauczycieli w Arundel High nie przeszkadzał mój zwyczaj ucinania sobie drzemek i dawali mi spokój, póki nie chrapałem, jednak było wśród nich również kilku okrutnych smutasów; ci za swój obowiązek uważali budzenie mnie – skrzypieniem kredy albo plaśnięciem gąbki do tablicy – i napadanie pytaniem: „A ty, Snowden, jak uważasz?”.

Podnosiłem wtedy głowę z blatu, prostowałem plecy, ziewałem i starałem się coś odpowiedzieć, podczas gdy moi koledzy i koleżanki z całych sił powstrzymywali się, by nie wybuchnąć śmiechem.

Jeśli mam być szczery, bardzo lubiłem te chwile, bo stanowiły jedno z największych wyzwań, jakie liceum miało mi do zaoferowania. Uwielbiałem to uczucie, kiedy ledwie wybudzony, oszołomiony, na oczach i uszach trzydziestu osób oczekujących mojej porażki przeczesywałem wzrokiem połowicznie zapisaną tablicę w poszukiwaniu jakiejś podpowiedzi. Wiedziałem, że jeśli wykażę się dostateczną przytomnością umysłu, by wymyślić dobrą odpowiedź, stanę się legendą, a jeśli nic nie przyjdzie mi na czas do głowy, zawsze będę mógł powiedzieć coś śmiesznego. Nigdy nie jest za późno na żart. W najgorszej możliwej sytuacji wybełkotałbym jakiś nonsens, a koledzy z klasy pomyśleliby, że jestem głupi. Nie przeszkadzało mi to. Nie należy wyprowadzać z błędu tych, którzy cię nie doceniają. Ci, co nie dostrzegają twojej prawdziwej wartości, obnażają tym samym własne wrażliwe punkty – ziejące dziury

w postrzeganiu świata, które powinny pozostać niezasklepione, jeśli chcesz przez nie później przegalopować na grzbiecie płonącego konia, by swym mieczem sprawiedliwości przywrócić prawdę.

Jako nastolatek byłem chyba odrobinę zbyt rozmiłowany w koncepcji, że najważniejsze sprawy w życiu mają charakter binarny, to znaczy, że określone podejście jest poprawne, a wszystkie pozostałe są błędne. Myślę, że dałem się omamić logice programowania komputerowego, gdzie na każde pytanie można odpowiedzieć wyłącznie na jeden z dwóch sposobów: „1” albo „0”; odpowiedzi te stanowią w kodzie maszynowym odpowiednik „tak” i „nie”, prawdy i fałszu. Logikę opozycji binarnej dawało się nawet stosować do pytań wielokrotnego wyboru na kartkówkach i sprawdzianach. Kiedy żadna z potencjalnych odpowiedzi nie rzucała mi się w oczy jako poprawna, mogłem ograniczyć liczbę możliwości poprzez eliminację, wypatrując terminów w rodzaju „zawsze” albo „nigdy” i szukając w myślach wyjątków, które je negowały.

Pod koniec pierwszej klasy liceum przyszło mi jednak zmierzyć się z wyzwaniem zupełnie innego rodzaju; nie było to pytanie, na które wystarczyło odpowiedzieć, poprawnie zakreślając kółko ołówkiem. Trzeba było posłużyć się umiejętnościami retorycznymi: napisać pełne zdania tworzące całe akapity. Mówiąc krótko, dostałem zadanie z angielskiego, a jego treść brzmiała: „Przygotuj tekst autobiograficzny o objętości co najmniej tysiąca słów”. Ktoś obcy nakazywał mi podzielić się przemyśleniami na chyba jedyny temat, na który nie miałem żadnych przemyśleń; chodziło o mnie, kimkolwiek byłem. Zwyczajnie nie potrafiłem tego zrobić. Doznałem kompletnej blokady. Nie oddałem wypracowania, a mój nauczyciel wpisał w dzienniku: zaległe.

Mój problem, podobnie jak temat pracy, był natury osobistej. Nie umiałem napisać wypracowania o charakterze autobiograficznym,

ponieważ w moim życiu panował zbyt duży chaos. Moja rodzina się rozpadała. Rodzice brali rozwód. Tato się wyprowadził, a mama wystawiła dom w Crofton na sprzedaż i przeniosła się wraz ze mną i siostrą do wynajmowanego mieszkania, a później do własnościowego lokalu na osiedlu w Ellicott City, pobliskim mieście. Jest takie znane powiedzenie, które słyszałem od kilku znajomych: naprawdę wchodzimy w dorosłość dopiero wtedy, gdy zostajemy rodzicami albo grzebiemy jednego z własnych. Nikt tymczasem nie wspomina, że dla dzieci w pewnym wieku rozwód rodziców jest takim doświadczeniem, jakby obie te rzeczy stały się jednocześnie. Nienaruszalne ikony twojego dzieciństwa znienacka przestają istnieć, a ich miejsce zajmuje – o ile w ogóle ktoś może je zająć – osoba zagubiona jeszcze bardziej niż ty, zalewająca się łzami i kipiąca z wściekłości, która pragnie od ciebie zapewnienia, że wszystko będzie dobrze. Ale nie będzie, w każdym razie nie od razu.

Podczas gdy sąd rozstrzygał o prawie do odwiedzin i opieki nad dziećmi, moja siostra rzuciła się w wir rekrutacji na studia, została przyjęta i zaczęła odliczać dni do wyjazdu; miała rozpocząć naukę na Uniwersytecie Karoliny Północnej w Wilmington. Wraz z jej wyjazdem traciłem najsilniejszą więź z moją rodziną w dawnej postaci.

Zareagowałem na te wydarzenia skupieniem na sobie. Zaparłem się i zmusiłem, by stać się inną osobą, aktorem zakładającym taką maskę, jaką potrzebowali w danej chwili widzieć ci, na których mi zależało. W otoczeniu rodziny grałem rolę szczerego i godnego zaufania. Przed przyjaciółmi – radosnego i beztroskiego. W samotności jednak stawałem się przygaszony, powiedziałbym, że wręcz wpadałem w posępny nastrój, i nieustannie zamartwiałem się, czy nie jestem dla innych ciężarem. Rozpamiętywałem wszystkie wycieczki samochodowe do Karoliny Północnej, gdy cały czas narzekałem, wszystkie Boże Narodzenia, których

nastrój popsułem kiepskimi świadectwami, wszystkie przypadki, kiedy odmówiłem wstania od komputera i wywiązania się z domowych obowiązków. Każdy dziecięcy bunt, na który sobie pozwoliłem, pojawiał się w mojej pamięci niczym migawki nagrania z miejsca zbrodni, dowód, że ponoszę odpowiedzialność za to, co się stało.

Próbowałem wyzbyć się poczucia winy, ignorując swoje emocje i pozorując samodzielność, aż zacząłem wydawać się otoczeniu przedwcześnie dojrzały. Zamiast mówić, że gram na komputerze, utrzymywałem, że na nim pracuję. Ta zamiana słów, mimo że nie zmieniłem niczego w sposobie spędzania czasu, sprawiła, że wszyscy – w tym nawet ja sam – zaczęli mnie postrzegać inaczej.

Przestałem mówić o sobie Eddie. Od tego momentu używałem imienia Ed. Dostałem swój pierwszy telefon komórkowy, który nosiłem – przypięty do paska – jak cholernie dorosły facet.

Dzięki temu, że trauma przyniosła mi nieoczekiwane błogosławieństwo – okazję do wymyślenia siebie na nowo – nauczyłem się doceniać świat poza czterema ścianami domu. Ku swemu zaskoczeniu odkryłem, że im większego dystansu nabierałem do obojga kochających mnie najbardziej na świecie dorosłych, tym bardziej zbliżałem się do innych, którzy traktowali mnie jak równego sobie. Do mentorów, którzy nauczyli mnie żeglować, walczyć i przemawiać publicznie, a nawet dali mi pewność siebie potrzebną, by stanąć na scenie. Wszystkie te osoby miały udział w moim wychowaniu.

Na początku drugiej klasy liceum zacząłem się szybciej męczyć i zapadać w sen częściej niż zwykle – już nie tylko na lekcjach, ale nawet przy komputerze. Zdarzało mi się budzić w środku nocy w pozycji mniej więcej siedzącej, naprzeciw ekranu zapisanego nonsensownymi znakami wskutek drzemki z głową na klawiaturze. Niedługo później zaczęły trapić

mnie bóle stawów, spuchły mi węzły chłonne, białka oczu przybrały żółty odcień i nie miałem siły wyjść z łóżka, nawet po dwunastu i więcej godzinach nieprzerwanego snu.

Po pobraniu sporej ilości krwi – nawet nie przypuszczałem, że mogę jej tyle w sobie mieć – zdiagnozowano u mnie mononukleozę zakaźną. Była to dla mnie choroba równie wycieńczająca, co wstydliwa, a to dlatego, że zwykle nabawia się jej poprzez zajęcie, które moi rówieśnicy nazywali chodzeniem ze sobą, tymczasem ja w wieku piętnastu lat miałem kontakty intymne co najwyżej metaforycznie, z moim modemem. Przestałem myśleć o szkole i zgromadziłem mnóstwo nieobecności, ale i to mnie nie cieszyło. Nie uszczęśliwiała mnie nawet dieta złożona wyłącznie z lodów. Z trudem znajdowałem energię na granie w gry, które otrzymywałem od rodziców – oboje starali się przynieść mi jak najfajniejszy, najnowszy tytuł, jakby konkurowali między sobą o to, kto mi bardziej poprawi humor, albo próbowali złagodzić swoje poczucie winy. Kiedy przestało mi się chcieć nawet poruszać joystickiem, zacząłem rozmyślać, po co w ogóle utrzymuję się przy życiu. Czasami budziłem się i nie rozpoznawałem, gdzie jestem. Potrzebowałem dłuższej chwili, by domyślić się, czy miałem przed oczami mrok mieszkania mojej mamy, czy kawalerki ojca, i nie pamiętałem, czy ktoś w ogóle przewoził mnie z jednego do drugiego. Każdy dzień wyglądał tak samo.

Żyłem jak we mgle. Pamiętam, że czytałem *The Hacker's Manifesto*, *Zamieć* Neala Stephensona i całe tomy J.R.R. Tolkiena; przy tym ostatnim zasypiałem w połowie rozdziału, mieszały mi się w głowie postaci i zdarzenia, aż zaczęło mi się śnić, że Gollum stoi przy moim łóżku i zawodzi: „Panie, Panie, informacje wolne chcą być".

Pogodziłem się z gorączkowymi urojeniami, które przynosił mi sen, ale trapił mnie jeden autentyczny koszmar; z nim nie potrafiłem sobie poradzić.

Była nim konieczność nadrobienia materiału szkolnego. Kiedy opuściłem mniej więcej cztery miesiące lekcji, otrzymałem z liceum Arundel High list informujący, że będę musiał powtórzyć drugą klasę. Chciałbym napisać, że mnie to zszokowało, ale kiedy tylko przeczytałem list, zdałem sobie sprawę, że od kilku tygodni z przerażeniem czekałem na tę wiadomość i wiedziałem, że jest nieunikniona. Nie wyobrażałem sobie, by wrócić do szkoły, nie mówiąc o powtarzaniu dwóch semestrów, i byłem gotów zrobić wszystko, co w mojej mocy, by tego uniknąć.

Wiadomość ta wybiła mnie z pełnoobjawowej depresji, w którą tymczasem przerodziła się moja gorączka gruczołowa. Z dnia na dzień stanąłem na nogi i po raz pierwszy od dawna założyłem na siebie coś innego niż piżamę. Praktycznie od razu zacząłem przeszukiwać internet i dzwonić w różne miejsca, szukając rozwiązań z pogranicza systemu, jakiegoś haku. Pogrzebałem tu i ówdzie i wypełniłem mnóstwo formularzy, po czym do mojej skrzynki pocztowej trafiło rozwiązanie: dostałem się do college'u. Okazało się, że do złożenia podania o przyjęcie nie był potrzebny dyplom ukończenia liceum.

Anne Arundel Community College był instytucją lokalną, w żadnym wypadku nie tak prestiżową jak uczelnia mojej siostry, jednak na moje potrzeby zupełnie wystarczającą. Ważne, że był akredytowany. Zaniosłem ofertę przyjęcia w poczet studentów do administracji mojego liceum, a ta z zaciekawieniem oraz nieskutecznie skrywaną mieszaniną rezygnacji i radości wyraziła zgodę na przeniesienie. Uczęszczałem na zajęcia w college'u dwa dni w tygodniu, czyli mniej więcej tyle, ile byłem w stanie utrzymać się w pozycji pionowej i normalnie funkcjonować, a dzięki temu, że zapisałem się na bardziej zaawansowane przedmioty, niż przerabiałem w liceum, nie musiałem męczyć się z materiałem z niezaliczonej klasy. Mogłem go po prostu pominąć.

College znajdował się mniej więcej dwadzieścia pięć minut jazdy samochodem od mojego domu i jako świeżo upieczony kierowca, który siłą woli zmuszał się, by nie zasnąć za kółkiem, trochę ryzykowałem, wybierając się do szkoły samodzielnie tych pierwszych kilka razy. Szedłem na zajęcia, a potem wracałem prosto do domu i kładłem się spać. Byłem najmłodszą osobą na wszystkich wykładach, możliwe, że też na uczelni. Niektórzy uważali mnie za ciekawostkę i coś na podobieństwo maskotki, u innych moja obecność wywoływała zmieszanie. W połączeniu z faktem, że wciąż się leczyłem, sprawiało to, że raczej nie nawiązywałem kontaktów towarzyskich. Poza tym do AACC się dojeżdżało, więc college nie mógł pochwalić się tętniącym życiem kampusem. Anonimowość, którą to zapewniało, mnie jednak odpowiadała, podobnie jak same zajęcia; większość z nich uważałem za zdecydowanie bardziej interesujące niż te, podczas których drzemałem w Arundel High.

Zanim przejdę dalej i raz na zawsze porzucę temat liceum, chciałbym zwrócić uwagę, że wciąż nie oddałem mojego zaległego zadania z angielskiego. Wypracowania autobiograficznego. Im jestem starszy, tym bardziej mi to ciąży, a pisanie na ten temat nie stało się ani trochę łatwiejsze.

W praktyce nikt, czyj życiorys wygląda podobnie jak mój, nie czuje się komfortowo, opowiadając o sobie. Trudno jest – spędziwszy tak wielką część życia na unikaniu identyfikacji – zupełnie zmienić podejście i dzielić się informacjami o charakterze osobistym za pośrednictwem książki. Służby wywiadowcze starają się wszczepić swoim pracownikom podstawowy poziom anonimowości, osobowość wypraną z cech rozpoznawczych, na którą nanosi się później to, czego wymagają dyskrecja i sztuka mistyfikacji. Szkolisz się, by nie zwracać na siebie uwagi, by

wyglądać i brzmieć jak inni. Mieszkasz w najzwyklejszym domu, jeździsz najzwyklejszym samochodem, nosisz te same ubrania co wszyscy. Jedyna różnica polega na tym, że robisz to celowo: normalność, przeciętność – to twoja przykrywka. Na tym polega przekora nagrody za oddanie się karierze, która wymaga wyparcia się siebie i nie przynosi publicznej chwały: osobistej satysfakcji nie osiąga się podczas pracy, lecz po jej zakończeniu, kiedy możesz wrócić do normalnego życia wśród ludzi i udaje ci się ich przekonać, że jesteś jednym z nich.

Istnieją dziesiątki popularniejszych i z pewnością trafniejszych terminów psychologicznych na to rozdwojenie tożsamości, ja jednak zwykłem nazywać je szyfrowaniem człowieka. Jak w każdym procesie szyfrowania pierwotny materiał – rdzeń twojej osobowości – wciąż istnieje, ale wyłącznie w niedostępnej i „przemieszanej" formie. Równanie, które umożliwia ten rodzaj kodowania, to prosta proporcjonalna zależność: im więcej wiesz o innych, tym mniej wiesz o sobie. Zdarza się, że w miarę upływu czasu zapominasz, co lubisz, albo nawet czego nie lubisz. Niektórzy tracą przekonania polityczne, a wraz z nimi wszelki szacunek do dowolnego systemu politycznego, choć wcześniej mu hołdowali. Pierwszeństwo przed wszystkim ma praca, ta zaś rozpoczyna się od wyparcia się własnej osobowości, a kończy wyparciem sumienia. Liczy się tylko misja.

Różne wersje tych przemyśleń służyły mi przez lata za wytłumaczenie, dlaczego z takim oddaniem dbałem o prywatność i czemu nie potrafiłem albo nie chciałem mówić o sprawach osobistych. Dopiero teraz, kiedy spędziłem poza społecznością wywiadowczą prawie tyle samo czasu, co w niej, zdaję sobie sprawę: to o wiele za mało. Przecież żaden był ze mnie szpieg – byłem jeszcze za młody, by się golić – kiedy nie oddałem wypracowania zadanego przez nauczyciela angielskiego. Jeśli już, to byłem

dzieciakiem, który od pewnego czasu uprawiał szpiegostwo – po części w formie eksperymentów sieciowych z tożsamościami przyjmowanymi przeze mnie w grach, ale głównie za sprawą wszystkich przemilczeń i kłamstw, z którymi musiałem sobie radzić w następstwie rozwodu rodziców.

Z chwilą, gdy doszło do tego rozłamu, zmieniliśmy się w rodzinę strażników tajemnic, mistrzów podstępu i kamuflażu. Rodzice zatajali różne rzeczy przed sobą, przede mną i moją siostrą. Siostra i ja z czasem zaczęliśmy mieć własne tajemnice, kiedy jedno spędzało weekend u ojca, a drugie u matki. Jednym z najbardziej przykrych doświadczeń, z którymi musi się mierzyć dziecko rozwodników, są przesłuchania prowadzone przez jednego rodzica na temat nowego życia drugiego.

Mama zaczęła spotykać się z innymi mężczyznami i znikała na dłużej. Ojciec starał się zapełnić pustkę najlepiej, jak potrafił, ale czasami nie umiał opanować wściekłości, którą wywoływał w nim przeciągający się i kosztowny proces rozwodowy. Za każdym razem, gdy mu się to przytrafiało, odnosiłem wrażenie, że nasze role się odwróciły. To ja musiałem wykazywać się asertywnością – stawiać mu czoła i apelować o rozsądek.

Przykro mi to pisać, aczkolwiek nie dlatego, że wydarzenia z tamtego okresu zostawiły w moim umyśle bolesne wspomnienia. Chodzi o rzecz zgoła odwrotną, o to, że epizody te w najmniejszym stopniu nie odzwierciedlały zasadniczo porządnego charakteru moich rodziców ani tej cechy, która po pewnym czasie pozwoliła im, z miłości do dzieci, zapomnieć o tym, co ich różniło, pogodzić się i we wzajemnym poszanowaniu, ale osobno, rozkwitnąć na nowo.

Tego rodzaju zmiany zachodzą u ludzi nieustannie i powszechnie. Wypracowanie o charakterze autobiograficznym jest tymczasem

statycznym, trwałym dokumentem opisującym ewoluującą osobę. Dlatego najlepszym sposobem, by opisać siebie, nie jest wymienianie faktów, lecz złożenie przysięgi w imię wyznawanych wartości i osoby, którą mamy nadzieję się stać.

Nie zapisałem się do lokalnego college'u, by kontynuować edukację akademicką, lecz aby oszczędzić czas po tym, jak spotkały mnie trudności. Przysiągłem sobie jednak, że zaliczę chociaż szkołę średnią. Udało mi się spełnić tę obietnicę w pewien weekend, kiedy pojechałem do publicznego liceum w okolicy Baltimore i podszedłem do ostatniego w życiu testu w stanie Maryland: egzaminu General Education Development (GED), który rząd Stanów Zjednoczonych traktuje na równi ze standardowym dyplomem ukończenia liceum.

Pamiętam, że gdy opuszczałem salę egzaminacyjną, towarzyszyło mi uczucie niezwykłej lekkości wywołane faktem, iż podchodząc do dwudniowego egzaminu, zaliczyłem dwa lata edukacji, które wciąż byłem winien stanowi. Czułem się, jakbym zhakował system, ale chodziło o coś więcej – o to, że dotrzymałem słowa danego samemu sobie.

07_11_września|

Mając szesnaście lat, byłem już praktycznie samodzielny. Mama rzuciła się w wir pracy i często zostawałem w jej przestronnym mieszkaniu sam, zatem ustalałem własny plan dnia, przygotowywałem sobie posiłki i prałem ubrania. Odpowiadałem za wszystko poza płaceniem rachunków.

Miałem hondę civic rocznik 92, którą jeździłem po całym stanie, słuchając alternatywnej stacji radiowej 99,1 WHFS – jednym z jej sloganów było „A teraz posłuchaj tego” – ponieważ tak robili wszyscy. Niezbyt dobrze radziłem sobie z byciem normalnym, ale się starałem.

Moje życie zaczęło toczyć się ustalonym torem, czas dzieliłem między dom, college i znajomych – spotykałem się przede wszystkim z nową grupą, którą poznałem na zajęciach z japońskiego. Nie jestem pewien, ile czasu potrzebowaliśmy, by zdać sobie sprawę, że utworzyliśmy klikę, ale podczas drugiego semestru przychodziliśmy na zajęcia nie tylko po to, by uczyć się języka, lecz by się zobaczyć. Jest to, nadmienię, najlepszy sposób, by robić wrażenie normalnego: otoczyć się osobami równie dziwnymi, a nawet dziwniejszymi od siebie. Większość koleżanek i kolegów z tej grupy aspirowała do miana artysty albo projektanta graficznego i miała obsesję na punkcie kontrowersyjnego jeszcze wówczas anime – japońskiej animacji. W miarę zacieśniania się naszych znajomości poszerzała się moja wiedza na temat różnych gatunków anime, aż osiągnąłem poziom, który pozwalał mi wygłaszać całkiem dojrzałe opinie na temat nowo odkrytych doświadczeń związanych z takimi tytułami jak *Grobowiec świetlików*, *Revolutionary Girl Utena*, *Neon Genesis Evangelion*, *Cowboy Bebop*,

Vision of Escaflowne, *Rurouni Kenshin*, *Nausicaä z Doliny Wiatru*, *Trigun*, *Magiczni wojownicy* i moim osobistym faworytem – *Ghost in the Shell*.

Jedną z nowych przyjaciółek była starsza ode mnie – znacznie starsza, wręcz całkiem już dorosła – dwudziestopięcioletnia kobieta, będę nazywał ją Mae. Jako artystka, której dzieła publikowano, i zapalona cosplayerka stanowiła swego rodzaju idolkę w oczach pozostałych członków naszej grupy. Była moją partnerką w konwersacjach na zajęciach z japońskiego oraz – co bardzo mi zaimponowało, kiedy to odkryłem – właścicielką wziętej firmy projektującej strony internetowe. Na potrzeby tej książki nazwę to przedsiębiorstwo Squirrelling Industries – od oswojonej latającej wiewiórki, którą Mae nosiła czasami w fioletowej filcowej torbie z logo whisky Crown Royal.

W ten oto sposób zostałem freelancerem: zacząłem pracować jako projektant stron internetowych dla dziewczyny, którą poznałem na zajęciach. Mae, czy może raczej jej firma, zatrudniła mnie na czarno za szczodrą jak na tamte czasy stawkę trzydziestu dolarów za godzinę, w gotówce. Rzecz rozbijała się o to, za ile godzin rzeczywiście mi zapłaci.

Mae oczywiście mogła wynagradzać mnie uśmiechem – bo byłem nią oczarowany, po prostu zakochany po uszy. I choć nie potrafiłem tego ukryć, wydaje mi się, że Mae nie miała mi tego za złe; nigdy nie spóźniałem się ze zleceniami i wykorzystywałem każdą, najdrobniejszą nawet okazję, by wyświadczyć jej jakąś przysługę. Poza tym szybko się uczyłem. W firmie, w której pracują dwie osoby, musisz umieć wszystko. Mimo że mogłem pracować dosłownie wszędzie – i korzystałem z tej możliwości, bo taki jest w końcu sens pracy w internecie – Mae wolała, żebym przyjeżdżał do biura, przez co miała na myśli swój dom: jednopiętrową kamienicę współdzieloną z mężem – zadbanym i inteligentnym mężczyzną, któremu dam na imię Norm.

Tak, Mae była mężatką. Co więcej, dom jednorodzinny, gdzie Mae mieszkała z Normem, mieścił się na południowo-zachodnim obrzeżu bazy Fort Meade, Norm pracował tam jako lingwista sił powietrznych z ramienia NSA. Nie potrafię powiedzieć, czy prowadzenie firmy z federalnego lokum umiejscowionego na terenie bazy wojskowej jest legalne, ale jako nastolatek zadurzony w zamężnej kobiecie, która przy okazji była moją szefową, nie uważałem za stosowne, by czepiać się takich drobnostek.

Obecnie jest to prawie nie do wyobrażenia, ale w tamtych czasach Ford Meade nie był naszpikowany słupkami drogowymi, barykadami i punktami kontrolnymi najeżonymi drutem kolczastym, lecz był niemal w całości dostępny dla każdego. Mogłem po prostu wjechać na teren bazy wojskowej mieszczącej jedną z najtajniejszych agencji wywiadowczych świata w moim civicu rocznik 92 z opuszczonymi oknami i radiem włączonym na cały regulator, nie zatrzymując się przed szlabanem i nie okazując dowodu tożsamości. Mniej więcej co drugi weekend jedna czwarta mojej grupy z japońskiego gromadziła się w niedużym domu Mae, który stał za siedzibą główną NSA, żeby oglądać anime i rysować komiksy. Takie po prostu były wtedy czasy – na każdym boisku szkolnym i w każdym sitcomie co rusz słyszało się wtedy retoryczne pytanie: „To chyba wolny kraj, prawda?”.

W dni robocze pojawiałem się u Mae rano, po wyjeździe jej męża do pracy. Parkowałem w ślepej uliczce przed ich domem i zostawałem na cały dzień, prawie do powrotu Norma. Gdy Norm i ja natykaliśmy się na siebie podczas dwóch lat, które przepracowałem dla jego żony, traktował mnie, jeśli zważyć na okoliczności, miło i serdecznie. Początkowo zakładałem, że nie zdaje sobie sprawy z mojego zauroczenia albo uważa prawdopodobieństwo uwiedzenia swojej żony przeze mnie za tak niskie, że nie ma nic przeciwko zostawianiu nas samych. Jednak pewnego dnia, gdy

mijaliśmy się na korytarzu – on wychodził, ja wchodziłem – uprzejmie zwrócił mi uwagę, że na stoliku nocnym trzyma pistolet.

Firma Squirrelling Industries, czyli w praktyce Mae i ja, działała jak jeden z wielu typowych garażowych start-upów zakładanych w okresie pierwszego boomu internetowego – małych przedsiębiorstw, które wydzierały sobie ochłapy, aż zawalił się cały rynek. Czekały, aż jakaś duża firma – na przykład producent samochodów – zatrudni poważną agencję reklamową albo firmę piarową, żeby stworzyła jej stronę internetową i ogólnie uatrakcyjniła sieciowy image. Duże firmy miały zerowe pojęcie o projektowaniu stron internetowych, natomiast poważne agencje reklamowe i firmy piarowe w najlepszym razie niewiele większe – wystarczające jednak, by zamieścić ogłoszenie o poszukiwaniu projektanta stron internetowych na jednym z portali dla freelancerów, które zyskiwały coraz większą popularność.

Drobne rodzinne firmy – a w naszym przypadku duet: mężatka i młody kawaler – stawały do przetargów, a olbrzymia konkurencja zmuszała je od proponowania niedorzecznie niskich stawek. Po odliczeniu honorarium, które zwycięski wykonawca musiał zapłacić portalowi z ogłoszeniami, z całego takiego kontraktu zostawała kwota z trudem zaspokajająca potrzeby jednej osoby, o rodzinie już nawet nie wspominając. Problemem nie był tylko brak satysfakcjonującej gratyfikacji finansowej – freelancerzy musieli też godzić się z brakiem uznania: najczęściej nie mogli wspominać, jakie projekty są ich dziełem, ponieważ agencje reklamowe i piarowe przypisywały ich autorstwo sobie i własnym zespołom informatycznym.

Pod okiem Mae nauczyłem się wiele o świecie, a w szczególności o realiach biznesowych. Była zaskakująco sprytna i pracowała dwa razy ciężej od innych, by odnieść sukces w branży, która w tamtych czasach zdecydowanie należała do mężczyzn, a co drugi klient naciągał

zleceniobiorców na pracę za darmo. Kultura swobodnego wyzysku zachęcała freelancerów do szukania na obrzeżach systemu sposobów, by go zhakować, a Mae miała talent do zarządzania swoimi relacjami, który pozwalał jej obchodzić portale pośredników. Starała się nie zadawać z osobami trzecimi i zawierać umowy bezpośrednio, wyłącznie z najpoważniejszymi klientami. Radziła sobie z tym wyśmienicie, szczególnie od momentu, gdy moja pomoc w kwestiach technicznych pozwoliła jej skoncentrować się w stu procentach na kwestiach biznesowej i artystycznej. Zrobiła dobry użytek ze swoich umiejętności ilustratorskich, projektując logotypy i oferując podstawowe usługi z zakresu zarządzania marką. Ja tymczasem odpowiadałem za metody i języki stosowane w projektowaniu stron, które były wystarczająco łatwe, bym mógł uczyć się ich na bieżąco, a na samą pracę, choć bywała brutalnie powtarzalna, nie narzekałem. Zabierałem się z uśmiechem za najnudniejsze nawet zajęcia w Notepadzie++. Niesamowite, do czego człowiek potrafi zmusić się z miłości, szczególnie gdy jest nieodwzajemniona.

Nie ukrywam, że ciekawi mnie, czy Mae od początku doskonale zdawała sobie sprawę z moich uczuć i po prostu wykorzystała je najlepiej, jak mogła. Jeśli jednak byłem ofiarą, to z własnej woli, a czas, który spędziłem jako jej podwładny, poprawił moją sytuację życiową.

Niezależnie od tego mniej więcej rok po rozpoczęciu pracy w Squirrelling Industries zdałem sobie sprawę, że muszę zacząć planować przyszłość. Coraz trudniej było mi ignorować znaczenie certyfikatów branżowych w sektorze informatycznym. W większości bardziej zaawansowanych ofert pracy i kontraktów zaczęło pojawiać się wymaganie, by kandydat był oficjalnie akredytowanym użytkownikiem i serwisantem produktów jednej z dużych firm technologicznych, na przykład IBM-a albo Cisco. Tak w każdym razie brzmiało przesłanie reklamy radiowej, którą

regularnie słyszałem w samochodzie. Pewnego dnia wróciłem z pracy i po wysłuchaniu tego spotu reklamowego po raz chyba setny zadzwoniłem pod podany numer z prefiksem 1–800 i zapisałem się na kurs certyfikacyjny Microsoftu oferowany przez Instytut Karier Komputerowych na Uniwersytecie Johnsa Hopkinsa. Przedsięwzięcie to, poczynając od nieprzyzwoicie wysokiej ceny po fakt, iż było ulokowane na terenie „kampusu pomocniczego” zamiast na głównym terenie uniwersytetu, zalatywało oszustwem, ale nie przejmowałem się. Cała sprawa miała charakter jawnie transakcyjny – Microsoftowi umożliwiała opodatkowanie prężnie rosnącego zapotrzebowania na informatyków, managerom HR udawanie, że kosztowny świstek papieru pozwala odróżnić autentycznych speców od parszywych ściemniaczy, a plebsowi mojego pokroju umieszczenie magicznych słów „Johns Hopkins” w CV i przeskoczenie na przód kolejki kandydatów.

Coraz to nowsze certyfikaty stawały się standardem w niemal tym samym tempie, w jakim branży udawało się je wymyślać. Akredytacja klasy A+ miała oznaczać, że potrafisz serwisować komputery. Certyfikat Net+ z kolei, że potrafiłeś rozwiązać podstawowe kwestie związane z administracją sieci. Żaden z nich nie dawał jednak szansy na nic więcej niż obsługa helpdesku. Najwartościowszymi świstkami papieru była seria certyfikatów Microsoftu; pierwszy z nich nosił nazwę Microsoft Certified Professional, MCP. Nad nim stał MCSA, czyli Microsoft Certified Systems Administrator, natomiast najwyżej cenionym papierkowym zaświadczeniem wiarygodności w dziedzinie technologii był MCSE, czyli Microsoft Certified Systems Engineer. Zdobycie tego ostatniego było jak wygranie głównej nagrody na strzelnicy w wesołym miasteczku. MCSE gwarantował źródło utrzymania. Absolutne minimum wynagrodzenia początkującego inżyniera z certyfikatem MCSE wynosiło 40 tysięcy

dolarów rocznie; była to kwota, która mnie – siedemnastolatkowi z przełomu stuleci – wydawała się oszałamiająca. Właściwie nie było w tym nic dziwnego. Przecież cena akcji Microsoftu wynosiła ponad sto dolarów, a Bill Gates został niedawno ogłoszony najbogatszym człowiekiem świata.

Pod względem wymaganej wiedzy technicznej certyfikat MCSE nie należał do najłatwiejszych do zdobycia, ale nie wymagał zdolności umysłowych, które mający szacunek do samego siebie haker nazwałby wybitnie genialnymi. Trzeba było jednak zaangażować znaczną ilość czasu i pieniędzy. Musiałem podejść do siedmiu testów, każdy kosztował sto pięćdziesiąt dolarów, i zapłacić mniej więcej osiemnaście tysięcy dolarów czesnego uniwersytetowi za pełny zestaw zajęć przygotowujących, których – jak na mnie przystało – nie ukończyłem, gdyż postanowiłem podejść do testów, kiedy tylko uznałem, że mam dość. Niestety Johns Hopkins nie zwracał pieniędzy za niewykorzystany czas lekcyjny.

Pożyczka, którą wziąłem na pokrycie kosztów nauczania, wymagała regularnych spłat, co dało mi bardziej praktyczny powód, by spędzać więcej czasu z Mae: zarobki. Poprosiłem o więcej godzin. Zgodziła się i zaproponowała, żebym zaczął przyjeżdżać o dziewiątej rano. To horrendalnie wczesna godzina, dla freelancera to już w ogóle, i dlatego właśnie w pewien wtorkowy poranek jechałem do pracy spóźniony.

Pędziłem drogą numer 32, nad głową miałem piękny, microsoftowy błękit nieba i starałem się nie wpaść w policyjne pułapki na kierowców przekraczających dozwoloną prędkość. Wiedziałem, że przy odrobinie szczęścia dotrę na dziewiątą trzydzieści i – jadąc z opuszczoną szybą i wystawionym łokciem – miałem wrażenie, że to będzie szczęśliwy dzień. Słuchałem mocno podgłośnionego radia i czekałem, aż skończą się wiadomości, a zacznie blok poświęcony sytuacji na drogach.

Właśnie miałem skręcić w skrót prowadzący do Fortu Meade przez Canine Road, kiedy przerwano audycję, by przekazać pilny komunikat o samolocie, który rozbił się w Nowym Jorku.

Mae otworzyła mi drzwi i ruszyłem za nią mrocznym przedsionkiem po schodach w górę, do ciasnego biura urządzonego w pokoju sąsiadującym z jej sypialnią. Było skromne: dwa biurka ustawione obok siebie, deska kreślarska, na której powstawały prace Mae, i klatka dla jej wiewiórek. To, co usłyszałem w wiadomościach, trochę mnie rozpraszało, ale mieliśmy pracę do wykonania, więc skupiłem się na obowiązkach. Zdążyłem otworzyć pliki projektu w zwykłym edytorze tekstowym – pisaliśmy kod stron internetowych ręcznie – kiedy zadzwonił telefon.

Mae podniosła słuchawkę.

– Co? Serio?

Przez to, że siedzieliśmy tak blisko siebie, słyszałem głos jej męża. Norm krzyczał.

Mae zrobiła zaniepokojoną minę i otworzyła na swoim komputerze portal z wiadomościami. Jedyny telewizor w domu znajdował się na parterze. Czytałem na tej samej stronie reportaż o samolocie, który uderzył w jedną z wież World Trade Center, kiedy Mae powiedziała do słuchawki:

– Okej. Wow. Okej – i odłożyła telefon. Odwróciła głowę w moją stronę. – Drugi samolot uderzył właśnie w drugą wieżę.

Do tego momentu sądziłem, że zdarzył się wypadek.

Mae stwierdziła:

– Norm jest zdania, że zamkną bazę.

– Masz na myśli główną bramę? – spytałem. – Serio? – Nie dotarła jeszcze do mnie waga tego, co się stało. Zastanawiałem się po prostu, jak wrócę do domu.

– Norm mówi, że powinieneś jechać. Nie chce, żebyś tu utknął.

Westchnąłem i zapisałem pracę, którą ledwie zdążyłem zacząć. Kiedy tylko zebrałem się do wyjścia, telefon odezwał się ponownie i tym razem rozmowa trwała jeszcze krócej. Mae zbladła.

– Nie uwierzysz, co się stało.

Pandemonium, chaos: pradawne, najbardziej pierwotne formy ludzkiego przerażenia. Oba te słowa odnoszą się do załamania porządku i fali paniki, która wdziera się w powstałą pustkę. Do końca życia będę pamiętał, jak po ataku na Pentagon wracałem do domu tą samą drogą, którą przyjechałem – mijając siedzibę główną NSA Canine Road. Z agencyjnych wieżowców pokrytych taflami czarnego szkła wylewało się szaleństwo, tsunami krzyków, dzwoniących telefonów komórkowych i samochodów na wysokich obrotach walczących o dostęp do wyjazdu z parkingu. W chwili najtragiczniejszego ataku terrorystycznego w historii Stanów Zjednoczonych tysiące członków personelu NSA – głównej amerykańskiej agencji wywiadu radiowego – porzucało swoje miejsce pracy, a ich powódź porwała również i mnie.

Dyrektor NSA, Michael Hayden, wydał rozkaz ewakuacji, zanim większość kraju zdążyła dowiedzieć się, co się stało. NSA i CIA – ta druga również ewakuowała 11 września wszystkich pracowników poza niezbędnym personelem – tłumaczyły swoje postępowanie niepokojem o to, że to właśnie któraś z agencji mogła – przypuszczalnie, potencjalnie, prawdopodobnie – być celem czwartego, ostatniego porwanego samolotu, lotu 93 United Airlines, a nie na przykład Biały Dom albo Kapitol.

Tymczasem ja wcale nie myślałem, co może być tym cholernym kolejnym celem, tylko brnąłem w ślimaczym tempie przez zakorkowany parking, który wszyscy usiłowali opuścić w tej samej chwili. Nie myślałem w ogóle o niczym. Posłusznie podążałem za innymi, starając się przetrwać moment; dziś wspominam to jako sumę wszystkich odbieranych wrażeń –

jazgotu klaksonów (chyba nigdy wcześniej nie słyszałem, by ktoś trąbił na terenie amerykańskiej instalacji wojskowej) i zgiełku niezsynchronizowanych odbiorników radiowych, wyjących na cały regulator o zawaleniu się południowej wieży, połączonego z widokiem ludzi ściskających kierownice kolanami i wciskających gorączkowo przycisk ponownego połączenia na swoich telefonach. Do dziś wciąż to czuję – zawsze jest tak, jakbym przenosił się do tamtych chwil – wrażenie emocjonalnej pustki za każdym razem, gdy przeciążona sieć komórkowa odrzucała moje połączenie, i stopniowo narastającą świadomość, że w tej sytuacji, odcięty od świata i zaklinowany zderzak w zderzak, mimo że siedziałem za kierownicą, byłem tylko pasażerem.

Sygnalizację świetlną na Canine Road zastąpili ludzie, a kierowanie ruchem przejęła specjalna policja NSA. Na przestrzeni kolejnych godzin, dni i tygodni do funkcjonariuszy dołączyły szpalery samochodów humvee z wieżyczkami wyposażonymi w karabiny maszynowe i zadaniem obrony nowo zainstalowanych blokad dróg i punktów kontrolnych. Wiele spośród tych środków bezpieczeństwa nabrało z czasem stałego charakteru; zostały potem uzupełnione o niezliczone metry drutu kolczastego i ogromne systemy kamer monitoringu. Po wprowadzeniu wszystkich tych zabezpieczeń nie mogłem już swobodnie jeździć do bazy i mijać siedziby NSA. Zmieniło się to dopiero w chwili, gdy zacząłem tam pracować.

Te pierwsze oznaki przedsięwzięcia, które później nazwano wojną z terroryzmem, nie były jedyną przyczyną, dlaczego po 11 września odpuściłem sobie Mae, choć z pewnością odegrały swoją rolę. Wydarzenia z tamtego dnia mocno nią wstrząsnęły. Po pewnym czasie przestałem dla niej pracować i oddaliliśmy się od siebie. Okazjonalnie próbowałem rozmawiać z nią przez internet, ale za każdym razem odkrywałem, że moje uczucia zmieniły się, ja zresztą też. Do czasu, gdy odeszła od Norma

i przeprowadziła się do Kalifornii, była dla mnie niemal kimś obcym. Za bardzo sprzeciwiała się wojnie.

08_12_września|

Spróbuj sobie przypomnieć największą rodzinną uroczystość, w jakiej zdarzyło ci się wziąć udział – na przykład rodzinny zjazd. Ile osób w nim uczestniczyło? Trzydzieści, pięćdziesiąt? Chociaż wszystkie są członkami twojej rodziny, być może nie miałeś okazji poznać każdej z nich bliżej. Zgodnie ze słynną liczbą Dunbara jesteśmy w stanie utrzymywać bliskie i trwałe relacje z maksymalnie stoma pięćdziesięcioma osobami. A teraz wróć pamięcią do szkolnych lat. Ilu uczniów liczyła twoja klasa w szkole podstawowej, a potem w średniej? Z iloma osobami ze szkoły naprawdę się przyjaźniłeś, z iloma po prostu się kolegowałeś, a ile znałeś jedynie z widzenia? Jeśli dorastałeś w Stanach Zjednoczonych, możemy przyjąć, że w sumie było ich około tysiąca. Zaliczenie ich wszystkich do grona twoich bliskich byłoby sporą przesadą, ale pewnie czujesz, że łączy cię z nimi pewna więź.

11 września 2001 roku zginęło prawie trzy tysiące ludzi. Pomyśl o wszystkich, których kochasz; o wszystkich, których poznałeś w ciągu swojego życia. Postaraj się przywołać z pamięci jak najwięcej znajomych imion, nazwisk i twarzy – a następnie pomyśl, że wszyscy ci ludzie nie żyją. Wyobraź sobie puste domy, opustoszałe klasy i szkolne korytarze. Jak byś się czuł, gdyby każda z będących częścią twojego życia osób nagle przestała istnieć? Wydarzenia 11 września pozostawiły po sobie niezatarte ślady. Pozostały po nich zarówno głębokie bruzdy w ziemi, jak i bolesne wyrwy w rodzinach i w lokalnych społecznościach.

Ale musimy uzmysłowić sobie coś jeszcze: amerykańska reakcja na tamte tragiczne wydarzenia pociągnęła za sobą ponad milion ofiar.

Droga, na którą wkroczyły Stany Zjednoczone po 11 września 2001 roku, okazała się nie tylko destrukcyjna, ale także autodestrukcyjna w skutkach; mimo to Ameryka podążała nią uparcie przez dwie kolejne dekady, realizując zakulisowe operacje, wprowadzając tajne ustawy, wytaczając niejawne procesy sądowe i tocząc sekretne wojny. Opłakane skutki wszystkich tych działań, a nawet sam fakt podejmowania tych środków, były utrzymywane w tajemnicy, dementowane, negowane i przeinaczane przez amerykańskie władze. Przepracowawszy mniej więcej połowę ostatniego dwudziestolecia w amerykańskich służbach wywiadowczych – drugą połowę tego okresu przyszło mi spędzić na przymusowej emigracji – lepiej niż większość ludzi zdaję sobie sprawę z tego, jak często służby specjalne popełniają błędy. Wiem również, że gromadzenie i analizowanie danych wywiadowczych może służyć uprawianiu dezinformacji i propagandy, których celem są nie tylko wrogowie Ameryki, ale także jej sojusznicy, a czasem nawet amerykańscy obywatele. A jednak pomimo całej mojej wiedzy na temat tych mechanizmów trudno mi jest pojąć i pogodzić się ze skalą oraz tempem zmiany, jaka dokonała się w Ameryce w ciągu ostatnich dwudziestu lat: z kraju, w którym fundamentalną zasadą było poszanowanie prawa każdego obywatela do wyrażania sprzeciwu wobec poczynań władzy, Stany Zjednoczone przedzierzgnęły się w państwo policyjne, gdzie zmilitaryzowana policja wymusza na obywatelu bezwarunkowe posłuszeństwo, mierząc do niego z broni palnej i wydając polecenie słyszane dziś na ulicach wszystkich amerykańskich miast: „Nie stawiaj oporu”.

Aby lepiej zrozumieć przyczyny tego, co zaszło w ciągu ostatnich dwóch dekad, wracam do września 2001 roku – do zamachów i ich bezpośrednich następstw. Wspominając wydarzenia tamtej jesieni, trzeba stawić czoło prawdzie bardziej ponurej niż kłamstwa o powiązaniach talibów z Al-Kaidą i o zapasach broni masowego rażenia, jakie rzekomo posiadał Saddam Husajn. Trzeba zmierzyć się z faktem, że rozlew krwi, bezprawne działania i nadużycia, jakie miały miejsce w tym samym czasie, kiedy wkraczałem w dorosłe życie, nie były wyłącznie rezultatem decyzji podejmowanych w gabinetach polityków i w kwaterach głównych tajnych służb, ale stanowiły także pokłosie tego, co działo się w sercach i umysłach wszystkich Amerykanów, nie wyłączając mnie samego.

Pamiętam, jak tuż po zawaleniu się północnej wieży World Trade Center przeciskałem się przez tłum szpiegów opuszczający w popłochu Fort Meade. Potem, podczas jazdy autostradą, jedną ręką trzymałem kierownicę, a drugą wybierałem numery na klawiaturze telefonu, bezskutecznie próbując dodzwonić się do moich bliskich. Wreszcie zdołałem połączyć się z mamą. Wówczas nie pracowała już w NSA; była urzędniczką sądową w siedzibie sądu federalnego w Baltimore. Dzięki temu uniknęła ewakuacji.

Zaniepokoiłem się, kiedy usłyszałem w słuchawce jej roztrzęsiony głos. Bardzo chciałem podnieść ją na duchu.

– U mnie wszystko w porządku, mamo. Właśnie wyjechałem z bazy – powiedziałem. – Nikogo z rodziny nie było dziś w Nowym Jorku, prawda?

– Ja… sama nie wiem. Nie mogę skontaktować się z babcią.

– A dziadek? Jest w Waszyngtonie?

– Wydaje mi się, że dziś mógł być w Pentagonie.

Poczułem, że nie mogę złapać tchu. W 2001 roku mój dziadek przeszedł ze Straży Wybrzeża do FBI, gdzie objął jedno z kierowniczych stanowisk

w biurze operacji lotniczych. Spędzał wiele czasu w siedzibach różnych federalnych agencji, rozsianych po Waszyngtonie i okolicy.

Zanim udało mi się wydusić z siebie jakieś słowa otuchy, ponownie odezwała się moja mama.

– Ktoś do mnie dzwoni. To może być babcia. Muszę kończyć.

Ponieważ mama długo nie oddzwaniała, próbowałem wielokrotnie wybierać jej numer, ale nie udało mi się z nią połączyć. Dojechałem więc do domu, usiadłem przed telewizorem i przeglądałem strony internetowych portali informacyjnych. Nasz nowy kablowy modem okazał się znacznie bardziej odporny na przeciążenia niż satelity telekomunikacyjne i stacje bazowe sieci komórkowej, które tamtego dnia szwankowały masowo w całym kraju.

Moja mama przedzierała się w tym czasie przez zakorkowane drogi. Kiedy w końcu przyjechała, była cała zapłakana, ale przynosiła dobre wieści. Mieliśmy szczęście: dziadek był w bezpiecznym miejscu.

Jakiś czas później spotkaliśmy się z dziadkami. Rozmawialiśmy o różnych rzeczach – o planach na Boże Narodzenie i o tym, jak spędzimy Nowy Rok – ale nie padło ani jedno słowo na temat ataków na budynek Pentagonu i na wieże WTC.

Mój tata z kolei chętnie dzielił się ze mną swoimi wspomnieniami z 11 września. Podczas ataku na WTC przebywał w kwaterze głównej Straży Wybrzeża. Wymknął się ze swojego biura w Departamencie Operacji i wraz z trzema innym oficerami wyruszyli na poszukiwanie wolnej sali konferencyjnej, w której mogliby obejrzeć nadawane w telewizji relacje na żywo. Na korytarzu natknęli się na pewnego młodego oficera, który mijając ich, rzucił: „Właśnie zbombardowali Pentagon”. Widząc niedowierzanie na twarzy mojego ojca i jego kolegów, powtórzył: „Nie żartuję, przed chwilą zbombardowali Pentagon”. Ojciec pospiesznie podszedł do szerokiego na

całą ścianę okna, skąd rozciągał się widok na drugi brzeg rzeki Potomak i na dwa z pięciu skrzydeł gmachu Pentagonu. Nad budynkiem unosiły się kłęby gęstego, czarnego dymu.

Im częściej tata wspominał tamtą sytuację, tym bardziej intrygowało mnie zdanie wypowiedziane przez młodego oficera: „Właśnie zbombardowali Pentagon”. Pamiętam, że za każdym razem zadawałem sobie w myślach pytanie: kim byli ci „oni”?

Ameryka natychmiast podzieliła świat na Nas i na Nich. Można było być albo z Nami, albo przeciwko Nam, jak ujął to prezydent Bush w swoim pamiętnym wystąpieniu wygłoszonym w czasie, gdy na zgliszczach zburzonych budynków tliły się jeszcze pożary. Nasi sąsiedzi wywiesili przed domami nowe amerykańskie flagi, jakby chcieli pokazać, po której są stronie. Ludzie kupowali papierowe kubki w kolorze czerwonym, białym i niebieskim, po czym wtykali je w oczka drucianej siatki okalającej estakady nad szosami i autostradami. Na odcinku drogi między domami mamy i ojca przyozdobiono w taki sposób każde ogrodzenie każdej estakady. Kolorowe kubki układały się w napisy w rodzaju UNITED WE STAND albo STAND TOGETHER NEVER FORGET („w jedności siła”, „bądźmy razem, nigdy nie zapominajmy”).

W tamtych czasach zdarzało mi się chodzić na strzelnicę. Obok klasycznych celów, czyli tarcz z siatką i kartonowych ludzkich sylwetek, pojawiły się nowe: podobizny mężczyzn w arabskich turbanach. Karabiny i pistolety, które całymi latami pokrywały się kurzem w gablotach sklepów z bronią, teraz schodziły na pniu. Amerykanie ruszyli też tłumnie do sklepów po telefony komórkowe, mając nadzieję, że dzięki nim otrzymają zawczasu ostrzeżenie o zbliżającym się ataku terrorystycznym albo przynajmniej będą mogli pożegnać się z bliskimi, gdyby mieli nieszczęście znaleźć się na pokładzie porwanego samolotu.

Dzień po zamachach niemal sto tysięcy szpiegów wróciło do pracy ze świadomością, że nie wywiązali się ze swojego najważniejszego zadania – ochrony Ameryki. Wyobraź sobie poczucie winy, jakie musiało ich z tego powodu dręczyć. Czuli ten sam gniew, co każdy Amerykanin, ale mieli jeszcze wyrzuty sumienia. Z oceną popełnionych przez nich błędów można było jednak poczekać. W tamtym momencie najważniejsze było, żeby się zrehabilitowali. Ich szefowie zajęli się tymczasem zabieganiem o przyznanie im dodatkowych środków z budżetu i szerszych kompetencji; wykorzystywali przy tym zagrożenie terrorystyczne do umocnienia swojej pozycji oraz dalszego zwiększenia zakresu uprawnień, który miał wykraczać poza najśmielsze oczekiwania nie tylko opinii publicznej, ale nawet tych, którzy ów nowy zakres zatwierdzali.

Dwunasty września 2001 roku był pierwszym dniem nowej ery, w którą Ameryka weszła zjednoczona i zdeterminowana, wzmocniona rozbudzonym patriotyzmem obywateli, a także życzliwością i sympatią świata. Z perspektywy czasu widać wyraźnie, że nasze państwo mogło lepiej wykorzystać tę szansę. Mogło potraktować terror nie jako zjawisko o podłożu religijnym, którym wydawał się być, tylko jako zbrodnię, którą był w rzeczywistości. Mogło zaprząc tę rzadką chwilę solidarności do służby na rzecz ugruntowania demokracji i skonsolidowania społeczeństwa połączonego teraz globalną siecią.

Zamiast tego Ameryka wyruszyła na wojnę.

Największym błędem, jaki popełniłem w życiu, było odruchowe i ślepe poparcie tego kroku. To prawda, byłem wtedy oburzony bezprzykładnymi aktami przemocy, jakie dokonały się 11 września, ale ten gniew stanowił zaledwie początek procesu, kiedy moje uczucia całkowicie wzięły górę nad racjonalnym osądem sytuacji. Przyjmowałem bezrefleksyjnie wszystkie stwierdzenia przedstawiane w mediach jako fakty; mało tego, powtarzałem

je tak gorliwie, jakby mi za to płacono. Chciałem być wyzwolicielem. Chciałem uwolnić uciśnionych od ciemiężycieli. Przyjąłem za pewnik prawdę skonstruowaną w interesie państwa, który pod wpływem targających mną emocji wziąłem mylnie za interes narodu. Było zupełnie tak, jakby cały mój dotychczasowy światopogląd legł nagle w gruzach – antyinstytucjonalny etos hakerski oraz apolityczny patriotyzm, który przejąłem od moich rodziców, zostały jakby wykasowane z mojego systemu, a ja przemieniłem się ochoczo w żywe narzędzie zemsty. Najbardziej zawstydzająca wydaje mi się dziś łatwość, z jaką dokonała się we mnie ta transformacja – i to, jak chętnie ją zaakceptowałem.

Sądzę, że pragnąłem być częścią czegoś większego. Przed 11 września byłem nastawiony sceptycznie do służby wojskowej, wtedy wydawała mi się pozbawiona sensu – albo zwyczajnie nudna. Każdy, kto spośród znanych mi osób służył w wojsku, zaciągnął się po zakończeniu zimnej wojny, po upadku muru berlińskiego i przed zamachami z 11 września. W tamtym okresie, który zbiegł się w czasie z moją młodością, Stany Zjednoczone nie miały wrogów. Kraj, gdzie dorastałem, był jedynym supermocarstwem; porządek świata oraz nasza pozycja wydawały się ustalone raz na zawsze – przynajmniej tak postrzegałem to ja i inni mi podobni. Nie widzieliśmy żadnych nowych, wielkich wyzwań, którym moglibyśmy stawić czoło, ani żadnych poważnych problemów, które moglibyśmy rozwiązać inaczej niż za pomocą internetu. Zamachy z 11 września wszystko zmieniły. W końcu rozgorzała walka, a my mogliśmy wziąć w niej udział.

Szybko poczułem się jednak rozczarowany możliwościami, jakie się przede mną otwierały. Uważałem, że najlepiej przysłużyłbym się ojczyźnie przy terminalu komputerowym, ale w nowej rzeczywistości asymetrycznego konfliktu normalna praca w sektorze IT wydawała mi się

zbyt wygodna i bezpieczna. Miałem nadzieję, że będę mógł robić to, co widuje się na filmach w scenach hakerskich pojedynków, gdy na ścianach z migoczących monitorów wyświetlają się ostrzeżenia o wirusach – chciałem namierzać wrogów Ameryki w sieci i udaremniać ich złowrogie plany. Niestety, wymagania dla kandydatów do pracy w NSA i CIA, czyli agencjach rządowych zajmujących się tego typu działaniami, sformułowano pół wieku wcześniej i do ubiegania się o większość stanowisk konieczne było posiadanie wyższego wykształcenia. Oznaczało to, że chociaż moje świadectwo ukończenia Anne Arundel Community College oraz certyfikat MCSE odpowiadały wymaganiom firm z branży technologicznej, to nie wystarczały do podjęcia pracy dla rządu. Im więcej jednak czytałem na ten temat w sieci, tym bardziej nabierałem przekonania, że w świecie po 11 września znacznie łatwiej było o wyjątki od rozmaitych reguł. Agencje rządowe rozrastały się tak szybko – dotyczyło to zwłaszcza ich pionów technicznych – że gotowe były przymykać oko na brak dyplomu wyższej uczelni w wypadku kandydatów, którzy odbyli służbę wojskową. To wtedy postanowiłem się zaciągnąć.

Biorąc pod uwagę militarne tradycje mojej rodziny, taka decyzja mogłaby się wydawać sensowna, a nawet nieunikniona. Lecz wcale tak nie było. Zaciągając się do wojska, w równym stopniu pozostawałem wierny rodzinnym tradycjom, co buntowałem się przeciw nim – ponieważ po rozmowach, jakie odbyłem w biurach rekrutacyjnych sił zbrojnych wszelkiego rodzaju, ostatecznie zdecydowałem się wstąpić do wojsk lądowych. Niektórzy członkowie mojej rodziny, przez całe życie związani ze Strażą Wybrzeża, uważali dowództwo amerykańskich wojsk lądowych za coś w rodzaju bandy szalonych wujaszków.

Mama, kiedy jej o wszystkim powiedziałem, przez kilka dni płakała. Wiedziałem, że lepiej nie wspominać o mojej decyzji ojcu, który już

wcześniej przy różnych okazjach dawał mi jasno do zrozumienia, że w wojsku jedynie zmarnowałbym swój techniczny talent. Tak czy inaczej, miałem już dwadzieścia lat; wiedziałem, co robię.

W dniu, kiedy wyjechałem na szkolenie, wsunąłem pod drzwi mieszkania ojca napisany odręcznie list, w którym wyjaśniałem powody mojej decyzji. Do dziś krzywię się z niesmakiem na samą myśl o ostatnim jego zdaniu. „Przepraszam, Tato – napisałem – ale to konieczne dla mojego osobistego rozwoju”.

09_Prześwietlenia|

Zaciągnąłem się do wojsk lądowych, ponieważ – zgodnie z ich rekrutacyjnym sloganem – chciałem być wszystkim, na co było mnie stać, a także dlatego, że nie chciałem służyć w Straży Wybrzeża. Poza tym dzięki dobrym wynikom uzyskanym na egzaminie wstępnym otworzyła się przede mną szansa na to, że od razu po ukończeniu szkolenia otrzymam stopień sierżanta i podejmę służbę w Siłach Specjalnych. Było to możliwe dzięki nowemu programowi szkoleniowemu, nazywanemu przez rekrutów 18 X-Ray*. Wprowadzono go w celu zaspokojenia rosnących potrzeb kadrowych niewielkich elitarnych jednostek amerykańskiej armii, na których spoczywał główny ciężar coraz bardziej tajnych operacji militarnych, prowadzonych przez Stany Zjednoczone w różnych zakątkach świata. Perspektywa udziału w tym programie była dla mnie nie lada gratką, tym bardziej że jeszcze całkiem niedawno, przed 11 września 2001 roku, do niezwykle wymagających testów kwalifikacyjnych do Sił Specjalnych dopuszczano wyłącznie żołnierzy czynnej służby. Nowy system pozwalał prześwietlić świeżo zrekrutowanych kandydatów do służby wojskowej i dokonać wstępnej selekcji polegającej na wyłowieniu spośród nich osób wyróżniających się sprawnością fizyczną, inteligencją oraz predyspozycjami do nauki języków obcych, czyli cechami, jakie musi posiadać każdy żołnierz jednostek specjalnych. Program 18 X-Ray gwarantował, że najbardziej obiecujący rekruci nie rozproszą się po różnych formacjach, tylko trafią od razu do Sił Specjalnych, które kusiły możliwościami zdobycia unikalnych umiejętności oraz szybkiego awansu

w wojskowej hierarchii. Żeby przygotować się do testów sprawnościowych, przez kilka miesięcy trenowałem biegi; nienawidziłem biegać, ale dzięki morderczym treningom nabrałem świetnej formy. W końcu zadzwonił do mnie pracownik wojskowego biura werbunkowego, gdzie zaciągnąłem się do służby; poinformował mnie, że zostałem przyjęty do programu 18 X-Ray. W jego głosie pobrzmiewały duma i radość – byłem pierwszym zwerbowanym przez niego rekrutem, który dostał się do tego programu. Powiedział, że po ukończeniu szkolenia zostanę prawdopodobnie awansowany do stopnia sierżanta łączności, sierżanta sapera lub sierżanta wywiadu Sił Specjalnych.

Prawdopodobnie.

Ale przedtem musiałem zaliczyć podstawowe szkolenie w Forcie Benning w stanie Georgia.

Całą podróż z Marylandu do Georgii odbytą autobusem, potem samolotem, a następnie znowu autobusem, siedziałem obok tego samego gościa – ogromnego kulturysty o napompowanych mięśniach, ważącego co najmniej dziewięćdziesiąt, a może i sto trzydzieści kilogramów. Usta nie zamykały mu się ani na chwilę: w kółko opowiadał o tym, jak strzeli w pysk każdego sierżanta instruktora, który spróbuje mu podskoczyć, a także udzielał mi wskazówek odnośnie cykli sterydowych i budowy masy mięśniowej. Trajkotał bez wytchnienia, dopóki nasz autobus nie dotarł do ośrodka szkoleniowego w Forcie Benning zwanego Sand Hill, czyli Piaskowym Wzgórzem – nawiasem mówiąc, piasku było tam raczej niewiele.

Sierżanci instruktorzy powitali nas furiackim wrzaskiem i natychmiast nadali wszystkim rekrutom przezwiska, kierując się przy tym naszymi pierwszymi drobnymi wpadkami i poważnymi błędami, takimi jak wyjście z autobusu w jaskrawej koszuli w kwiatowe wzory albo posiadanie

nazwiska, które łatwo było przekręcić w zabawny sposób. Tak oto zostałem Śnieżynką (Snowflake), a mojego potężnie zbudowanego towarzysza podróży ochrzczono Stokrotką. Jedyne, co mógł zrobić, to zacisnąć zęby – nikt z nas nie odważyłby się zacisnąć pięści – i zżymać się w milczeniu.

Nasi instruktorzy szybko się zorientowali, że Stokrotka i ja zdążyliśmy zaznajomić się w trakcie podróży; ich uwadze nie uszedł także fakt, że byłem najchudszym rekrutem w całym plutonie – ważyłem 57 kilogramów przy wzroście 180 centymetrów – a Stokrotka był z nas wszystkich najcięższy. Instruktorzy postanowili zabawić się naszym kosztem, dobierając nas w parę tak często, jak tylko było to możliwe. Wciąż pamiętam ćwiczenie polegające na przenoszeniu rzekomo rannego partnera na odległość około stu metrów, z wykorzystaniem rozmaitych metod: czołgania z chwytem za kark, chwytu strażackiego czy szczególnie komicznego chwytu kołyskowego, przypominającego przenoszenie przez próg panny młodej. Kiedy to ja musiałem nieść Stokrotkę, nie było mnie widać spod jego cielska. Ktoś mógłby pomyśleć, że Stokrotka unosi się w powietrzu – w rzeczywistości jednak podtrzymywałem go ja, pocąc się i klnąc na czym świat stoi. Robiłem, co w mojej mocy, żeby dotaszczyć jego gigantyczny zad do wyznaczonego punktu, zanim padnę pod jego ciężarem. Po dotarciu na metę Stokrotka zrywał się ze śmiechem na równe nogi i przewieszał mnie sobie przez szyję niczym mokry ręcznik, po czym w podskokach przebiegał cały dystans, którego pokonanie kosztowało mnie tyle wysiłku.

Chodziliśmy stale brudni i obolali, ale po paru tygodniach od rozpoczęcia szkolenia byłem w najlepszej kondycji w całym moim życiu. Moja drobna budowa, choć początkowo wydawała mi się przekleństwem, wkrótce okazała się atutem, ponieważ wiele wykonywanych przez nas ćwiczeń wymagało dźwigania ciężaru własnego ciała. Stokrotka nie radził

sobie ze wspinaniem się po linie, po której ja śmigałem niczym wiewiórka. Miał problem z wykonaniem minimalnej liczby podciągnięć na drążku, podczas gdy ja nawet na jednej ręce robiłem ich dwa razy więcej, niż wynosiło ustalone minimum. Po zrobieniu kilku pompek Stokrotka oblewał się potem, natomiast ja potrafiłem robić je z klaśnięciem albo podpierając się tylko jednym kciukiem. Kiedy instruktorzy urządzili nam test sprawdzający, ile pompek zdołamy wykonać w dwie minuty, przerwali mi przed upływem tego czasu, bo osiągnąłem najlepszy przewidziany w tabeli wynik.

Prawie zawsze i wszędzie poruszaliśmy się szybkim marszem – albo biegiem. Biegaliśmy na okrągło. Przed posiłkami i po posiłkach; po drogach, po polach i po bieżni, powtarzając za sierżantem instruktorem kolejne wersy marszowych przyśpiewek:

Na pustynię się udałem,
Gdzie grasują terroryści,
Mam maczetę i karabin,
Co ma być, niech się ziści.

Lewa, prawa, lewa, prawa – zabijemy, zabijemy!
Nie podskakuj, bo wiesz dobrze, że zrobimy, co umiemy!

Wyprawiłem się do jaskiń,
Gdzie się kryją terroryści,
Granat wziąłem i rzuciłem,
Co ma być, niech się ziści.

Lewa, prawa, lewa, prawa – zabijemy, zabijemy!
Nie podskakuj, bo wiesz dobrze, że zrobimy, co umiemy!

Bieg w zwartej grupie i monotonny, rytmiczny zaśpiew działają usypiająco; sprawiają, że czujesz się tak, jakbyś wychodził poza siebie. W uszach dudni ci głos kilkudziesięciu mężczyzn wyrzucających z siebie te same słowa, co ty. Twój wzrok utkwiony jest w stopach biegnącego przed tobą kolegi. Po jakimś czasie przestajesz myśleć; masz wrażenie, że stopniowo rozpływasz się i zlewasz w jedno ze swoim oddziałem. Można by stwierdzić, że na swój sposób było to relaksujące doświadczenie, gdyby nie poczucie zupełnego otępienia. Można by powiedzieć, że bieg mnie uspokajał, gdyby nie to, że byłem skrajnie wyczerpany. Właśnie taki był cel tych ćwiczeń. Poniewierani rekruci nie policzkują swoich instruktorów musztry nie dlatego, że powstrzymuje ich strach przed konsekwencjami, ale dlatego, że są zbyt wycieńczeni: zwyczajnie szkoda im na to fatygi. Wojsko zaczyna kształtować swoich żołnierzy od odebrania im chęci do walki – mają ćwiczyć tak długo, aż będą zbyt zmęczeni, by chciało im się robić cokolwiek poza wykonywaniem rozkazów.

Na odrobinę wytchnienia mogliśmy liczyć wyłącznie nocą, w koszarach – najpierw jednak musieliśmy sobie zapracować na ten przywilej, ustawiając się w szeregu przed pryczami i recytując credo amerykańskiego żołnierza, a następnie śpiewając *Gwiaździsty sztandar*. Stokrotka notorycznie zapominał słów hymnu, a do tego ewidentnie słoń nadepnął mu na ucho.

Niektórzy z moich kolegów jeszcze długo po capstrzyku rozprawiali o tym, co zrobią z bin Ladenem, kiedy już go złapią. Żaden nie miał wątpliwości, że tak się stanie. Większość ich fantazji krążyła wokół dekapitacji, kastracji albo napalonych wielbłądów. Ja z kolei regularnie śniłem o tym, że biegam – ale nie przez porośnięte bujną roślinnością przestrzenie Georgii, tylko po pustyni.

W trzecim lub czwartym tygodniu szkolenia odbyły się ćwiczenia z orientacji i poruszania się w terenie. Nasz pluton miał odbyć długi marsz w trudnych warunkach, wymagających wspinania się na ogromne głazy i przekraczania w bród strumieni; wyznaczona przez instruktorów trasa biegła przez leśne ostępy, a my mieliśmy do dyspozycji jedynie mapę i kompas – nie mogliśmy korzystać z GPS-ów ani z innych cyfrowych pomocy. Wykonywaliśmy już wcześniej podobne ćwiczenia, ale tym razem po raz pierwszy mieliśmy maszerować w pełnym oporządzeniu, z plecakami wypełnionymi ekwipunkiem ważącym około dwudziestu kilogramów. Jakby tego było mało, buty, w które wyposażyła mnie amerykańska armia, były tak szerokie, że stopy przesuwały mi się w nich swobodnie we wszystkie strony. Szybko poczułem, że moje palce u stóp zaczynają pokrywać się pęcherzami.

W połowie dystansu przypadła moja kolej na prowadzenie oddziału. Wdrapałem się na powalone przez burzę drzewo, jego pień wisiał nad leśną ścieżką mniej więcej na wysokości mojej klatki piersiowej. Wyznaczyłem azymut i sprawdziłem na mapie nasze położenie. Ustaliłem, że nie zboczyliśmy z trasy, po czym chciałem zeskoczyć na ziemię. Zdążyłem już wysunąć przed siebie jedną nogę, gdy zauważyłem zwiniętego w kłębek węża, leżącego na ścieżce dokładnie tam, gdzie zamierzałem postawić stopę. Nie jestem znawcą przyrody, dlatego nie potrafię powiedzieć, do jakiego gatunku należało to stworzenie. Niespecjalnie mnie to zresztą obchodziło. Dzieci w Karolinie Północnej uczy się, że wszystkie węże są śmiertelnie niebezpieczne, a ja nie zamierzałem sprawdzać tego na własnej skórze.

Wykonałem więc coś w rodzaju próby powietrznego spaceru. Wysunąłem zawieszoną w powietrzu nogę do przodu, a potem jeszcze nieco dalej, wyciągając przy tym lekko stopę, by zyskać kilka dodatkowych

centymetrów, gdy nagle zdałem sobie sprawę, że spadam. Kiedy moje stopy dotknęły ziemi – w pewnej odległości od węża – poczułem w obu nogach palący ból, jakiego nie wywołałoby ukąszenie nawet najbardziej jadowitej żmii. Zrobiłem kilka chwiejnych kroków, żeby złapać równowagę, i już wiedziałem, że coś jest nie w porządku. Bardzo nie w porządku. Ból w nogach był potworny, ale nie mogłem po prostu się zatrzymać; musiałem iść dalej, bo byłem w wojsku, a wojsko – akurat w samym środku lasu. Zebrałem całą siłę woli, jaką zdołałem z siebie wykrzesać, i spróbowałem wyprzeć ból ze świadomości, skupiając się na utrzymaniu stałego rytmu kroków: lewa, prawa, lewa, prawa.

Szło mi się coraz trudniej i chociaż ostatecznie ukończyłem marsz, to dokonałem tego tylko dlatego, że nie miałem innego wyjścia. Kiedy dotarłem do koszar, moje nogi były zupełnie odrętwiałe. Zajmowałem górne łóżko albo, jak kto woli, pryczę i wdrapanie się na nią okazało się sporym problemem. Musiałem złapać za ramę łóżka, a następnie podźwignąć się na rękach tak, jakbym gramolił się z wody na brzeg basenu; dopiero kiedy mój tułów znalazł się już na materacu, wciągnąłem na górę zdrętwiałe dolne kończyny.

Następnego dnia rano z niespokojnego snu wyrwał mnie hałaśliwy brzęk metalowej puszki ciśniętej z impetem o podłogę sali – taka pobudka oznaczała, że ktoś z nas nie wypełnił swoich obowiązków w satysfakcjonujący sierżanta sposób. Poderwałem się odruchowo i zeskoczyłem z łóżka. Kiedy wylądowałem na dole, moje nogi odmówiły posłuszeństwa. Ugięły się pode mną kolana i chwilę potem leżałem jak długi.

Próbowałem wstać, chwytając oburącz za dolną pryczę, żeby powtórzyć numer z podciągnięciem się na rękach, ale gdy tylko poruszyłem nogami,

wszystkie mięśnie mojego ciała przeszył gwałtowny ból. Opadłem bezsilnie na ziemię.

Wokół mnie zdążył zebrać się tłumek kolegów. Początkowo obserwowali moje nieporadne wysiłki ze śmiechem, który szybko ustąpił jednak miejsca głosom zaniepokojenia, a potem milczeniu, jakie zapadło w pomieszczeniu, gdy zbliżył się do mnie sierżant.

– Co się z tobą dzieje, złamasie? – zapytał. – Wstawaj z mojej podłogi, zanim cię w nią wdepczę.

Momentalnie i nierozsądnie spróbowałem wykonać jego polecenie. Kiedy sierżant dostrzegł bolesny grymas na mojej twarzy, powstrzymał mnie, opierając rękę na mojej piersi.

– Stokrotka! Zaniesiesz Śnieżynkę do lazaretu – polecił, a następnie nachylił się nade mną, tak jakby nie chciał, żeby inni usłyszeli jego łagodny ton głosu. – Słuchajcie, szeregowy. Kiedy tylko otworzą gabinet lekarski, weźmiecie kule i natychmiast zawleczecie tam swoje połamane dupsko.

W wojsku do wszelkich kontuzji i obrażeń podchodzi się z dużą dozą nieufności, głównie dlatego, że armia stawia sobie za cel wyrobienie w żołnierzach przekonania o własnej niezniszczalności, ale także dlatego, że chce uniknąć oskarżeń o błędy popełnione w procesie szkolenia. W rezultacie niemal każdy, kto uskarża się na kontuzję odniesioną podczas ćwiczeń, traktowany jest jak mazgaj albo jeszcze gorzej – jak symulant.

Stokrotka zaniósł mnie do lazaretu, a potem musiał mnie opuścić. Był zdrowy i dlatego należało go izolować od tych, którzy zgłaszali jakieś dolegliwości. Byliśmy niczym kasta nietykalnych, jak trędowaci – żołnierze niezdolni do udziału w szkoleniu z powodu skręconych kostek, ran szarpanych, oparzeń, złamanych kończyn albo martwicy tkanek wywołanej jadem pająka. To właśnie z tego okrytego hańbą grona mieli się wywodzić moi nowi *battle buddies*. *Battle buddy* to twój partner – kompan – który ma

podążać za tobą niczym cień, zwłaszcza jeśli zachodzi najmniejsze nawet ryzyko, że tam, dokąd się wybierasz, mógłbyś być sam. Kiedy człowiek jest sam, może zacząć myśleć, a w wojsku wychodzi się z założenia, że myślenie to prosta droga do kłopotów.

Moim nowym kompanem został bystry przystojniak, były fotomodel w typie Kapitana Ameryki. Mniej więcej tydzień wcześniej doznał kontuzji biodra, ale zgłosił to dopiero wtedy, gdy ból stał się nie do zniesienia, i teraz tak jak ja musiał poruszać się o kulach. Żaden z nas nie był w nastroju do rozmowy, dlatego kuśtykaliśmy jeden obok drugiego w ponurym milczeniu – lewa, prawa, lewa, prawa, w równym, chociaż ślamazarnym tempie. W szpitalu zostałem prześwietlony i dowiedziałem się, że doznałem obustronnego pęknięcia kości piszczelowych. Są to pęknięcia przeciążeniowe; powstałe na powierzchni kości szczeliny mogą z czasem pogłębić się aż do szpiku kostnego. Jedynym sposobem na zapobieżenie takim powikłaniom i przyspieszenie regeneracji kości było unikanie chodzenia. Po wydaniu diagnozy kazano mi wracać do mojego batalionu.

Tyle tylko, że nie mogłem się tam udać bez mojego kompana, który udał się na prześwietlenie zaraz po mnie i nie wyszedł jeszcze z gabinetu. Doszedłem do wniosku, że lekarze nadal go badają, więc uzbroiłem się w cierpliwość i czekałem. I czekałem. Mijały godziny. Zabijałem czas, czytając gazety i czasopisma – był to luksus, na który w normalnych okolicznościach nie mógł sobie pozwolić żaden uczestnik podstawowego szkolenia.

W końcu podeszła do mnie pielęgniarka i poprosiła, żebym udał się do recepcji: dzwonił mój sierżant instruktor. Kiedy dokuśtykałem do telefonu, usłyszałem w słuchawce wściekły głos sierżanta.

– Jak tam, Śnieżynka, znalazłeś sobie jakąś ciekawą lekturę? Skoro już tam jesteś, może zorganizujesz trochę puddingu i kilka egzemplarzy „Cosmo” dla dziewczyn? Do diabła, dlaczego ty i ta druga szumowina jeszcze nie wróciliście?!

– Panie sierżancie, ciągle czekam na mojego kompana.

– A gdzie on się, kurwa, podziewa, co?!

– Nie wiem, panie sierżancie. Wszedł do gabinetu i jeszcze stamtąd nie wyszedł, panie sierżancie.

Sierżant nie był zadowolony z mojej odpowiedzi.

– To rusz tę swoją kaleką dupę – wrzasnął jeszcze głośniej – i idź go poszukaj, do cholery!

Pokuśtykałem do rejestracji, żeby zasięgnąć języka. Powiedziano mi, że mój kompan przechodzi właśnie operację.

Dopiero pod wieczór, po kilku telefonicznych rozmowach z coraz bardziej zdenerwowanym sierżantem, udało mi się wreszcie dowiedzieć, co dokładnie stało się z moim towarzyszem. Okazało się, że mój kompan przez tydzień chodził ze złamanym biodrem i gdyby nie natychmiastowa operacja, podczas której skręcono śrubami jego pogruchotaną kość, mógłby zostać kaleką do końca życia. Zachodziło poważne ryzyko uszkodzenia głównych nerwów, ponieważ złamane fragmenty kości były ostre niczym brzytwa.

Ostatecznie wróciłem do Fortu Benning w pojedynkę, po czym trafiłem z powrotem do lazaretu. Każdemu, kto spędził w wojskowej lecznicy więcej niż trzy lub cztery dni, groziło poddanie „recyklingowi” – co oznaczało konieczność rozpoczęcia od początku szkolenia podstawowego – albo, co gorsza, przeniesienie do szpitala, a w konsekwencji zwolnienie ze służby i odesłanie do domu. Dla wielu przebywających w lazarecie pechowców służba w wojsku była tak naprawdę jedynym rozwiązaniem,

jedyną szansą na wyrwanie się z patologicznej rodziny albo na uniknięcie pozbawionej perspektyw pracy, jaką musieliby wykonywać w cywilu – a teraz groziło im przymusowe zakończenie służby wojskowej, w dodatku z nieodwracalnie zniszczonym zdrowiem.

Byliśmy niepotrzebnymi wojsku wyrzutkami, małą armią powłóczących nogami kalek, a naszym jedynym zajęciem było wysiadywanie na ławeczkach dwanaście godzin dziennie. Nasze urazy i kontuzje sprawiały, że byliśmy niezdolni do służby, i dlatego trzeba nas było odseparować od naszych zdrowych kolegów, tak jakby instruktorzy obawiali się, że zarazimy ich naszą słabością lub niebezpiecznymi pomysłami, jakie mogły przyjść nam do głowy podczas godzin spędzanych bezczynnie na ławce. Nie dość, że musieliśmy znosić fizyczne cierpienie wywołane odniesionymi obrażeniami, to pozbawiano nas nawet takich drobnych uciech jak obejrzenie pokazu fajerwerków z okazji Dnia Niepodległości. W czasie wieczornego pokazu pełniliśmy „dyżur przeciwpożarowy” polegający na pilnowaniu, czy w opustoszałych koszarach nie wybuchnie przypadkiem pożar.

Wartowaliśmy dwójkami. Stałem w ciemnościach, wsparty na kulach, i udawałem, że robię coś pożytecznego. Obok mnie tkwił mój towarzysz: miły, prosty chłopak, muskularny osiemnastolatek, który trafił do lazaretu z dość podejrzanymi obrażeniami, mogącymi być wynikiem samookaleczenia. Jak sam stwierdził, w ogóle nie powinien zaciągać się do wojska. W oddali strzelały fajerwerki, a on opowiadał mi o tym, jak wielki to był błąd, jak bardzo czuł się samotny i jak okropnie doskwierała mu tęsknota za rodzicami i domem – rodzinną farmą gdzieś w Appalachach.

Współczułem mu, ale niewiele mogłem dla niego zrobić. Zachęciłem go, żeby porozmawiał z kapelanem.

– Zagryź zęby – poradziłem. – Z czasem przywykniesz i może wtedy poczujesz się lepiej.

Ale on stanął przede mną i w rozbrajająco dziecinny sposób oświadczył, że zamierza uciec do domu – w wojsku samowolne oddalenie się z jednostki stanowi poważne przestępstwo – po czym zapytał, czy zamierzam komuś o tym powiedzieć. Dopiero wtedy zauważyłem, że ma przy sobie worek na rzeczy do prania. Naprawdę zamierzał uciec i to właśnie teraz.

Nie wiedziałem, jak mam się zachować. Spróbowałem przemówić mu do rozsądku. Ostrzegłem go, że dezercja to fatalny pomysł, że będzie ścigany prawem i przez resztę życia będzie się musiał liczyć z tym, że każdy policjant w kraju może go aresztować. On jednak pokręcił głową. Stwierdził, że tam, gdzie mieszka, daleko w górach, nie ma żadnych policjantów. Dodał, że to jego ostatnia szansa na odzyskanie wolności.

Zrozumiałem, że podjął już decyzję i nie zamierza jej zmienić. W przeciwieństwie do mnie nie poruszał się o kulach, a do tego był ode mnie znacznie większy. Gdyby rzucił się do ucieczki, nie miałbym szans go dogonić; gdybym próbował powstrzymać go siłą, rozerwałby mnie na strzępy. Jedyne, co mogłem zrobić, to donieść na niego przełożonym – ale gdybym to zrobił, sam naraziłbym się na karę za to, że kontynuowałem tę rozmowę zamiast od razu wezwać posiłki i sprać niedoszłego dezertera moją kulą.

Ogarnął mnie gniew. Po chwili zdałem sobie sprawę, że wrzeszczę na stojącego przede mną chłopaka. Dopytywałem, dlaczego nie poczekał, aż pójdę do latryny, i nie zwiał po cichu? Dlaczego postawił mnie w takiej sytuacji?

– Bo tylko ty słuchasz – odparł miękko, a potem się rozpłakał.

Najsmutniejsze w tym wszystkim było to, że miał rację. Otaczało go stale dwustu pięćdziesięciu mężczyzn, a mimo to czuł się zupełnie sam. Przez moment obaj milczeliśmy; w oddali wybuchały z hukiem sztuczne ognie. W końcu westchnąłem i powiedziałem:

– Muszę iść do latryny. Zajmie mi to jakiś czas.

Potem pokuśtykałem w swoją stronę, nie oglądając się za siebie.

Nigdy więcej go nie zobaczyłem. Myślę, że to właśnie wtedy uświadomiłem sobie, że ja również wcale nie chcę zostać w wojsku.

Moja następna wizyta lekarska tylko mnie w tym utwierdziła.

Lekarz, do którego tym razem trafiłem, był wysokim, tyczkowatym Południowcem o ironicznym usposobieniu. Przebadał mnie i przyjrzał się nowym zdjęciom rentgenowskim moich kości, po czym orzekł, że nie jestem w stanie kontynuować służby w kompanii. Następnym etapem było szkolenie spadochronowe, a on postawił sprawę jasno: „Synu, jeśli po skoku wylądujesz na tych nogach, to obie rozsypią się w proch”.

Ogarnęło mnie przygnębienie. Nieukończenie w terminie podstawowego szkolenia skutkowało skreśleniem z listy uczestników programu 18X – a to z kolei oznaczało, że mogłem zostać przeniesiony do jakiejkolwiek formacji na dowolne stanowisko, zależnie od aktualnych potrzeb wojska. Mogli zrobić ze mnie zwykłego piechura, mechanika lub kancelistę, mogli też skierować mnie do pracy w kuchni przy obieraniu ziemniaków albo – i tego obawiałem się najbardziej – powierzyć mi stanowisko specjalisty od komputerów w wojskowym biurze wsparcia technicznego.

Lekarz musiał zauważyć moją niewesołą minę, bo odchrząknął i przedstawił mi dwie możliwości: mogłem albo zostać „zrecyklingowany” i czekać na nowy przydział, albo skorzystać z jego rekomendacji, żeby zastosować wobec mnie procedurę zwaną „administracyjnym zwolnieniem

ze służby wojskowej”. Wyjaśnił, że jest to szczególny rodzaj odprawienia z wojska, które nie jest klasyfikowane ani jako honorowe, ani jako niehonorowe, i ma zastosowanie wyłącznie w stosunku do żołnierzy służących krócej niż sześć miesięcy. Bardziej przypominało to decyzję o anulowaniu małżeństwa niż rozwód, a sama procedura przebiegała stosunkowo szybko.

Przyznaję, że spodobał mi się ten pomysł. Przez głowę przemknęła mi nawet myśl, że jest to swoista karmiczna nagroda za miłosierdzie okazane dezerterowi z Appalachów. Lekarz dał mi czas na zastanowienie się, a kiedy wrócił po godzinie, przyjąłem jego propozycję.

Wkrótce potem zostałem przeniesiony do szpitala wojskowego, gdzie zakomunikowano mi, że chcąc skorzystać z administracyjnego zwolnienia ze służby, muszę podpisać oświadczenie, że mój stan zdrowia uległ całkowitej poprawie, a złamania zostały wyleczone. Mój podpis był niezbędny, ale rzekomo była to czysta formalność. Kilka gryzmołów i będę wolny.

Trzymając kartkę z oświadczeniem w jednej ręce, a długopis w drugiej, uśmiechnąłem się pod nosem. Zrozumiałem, gdzie tkwił haczyk: to, co wziąłem początkowo za wspaniałomyślną ofertę życzliwego i troskliwego lekarza wojskowego, było tak naprawdę wybiegiem; rząd chciał uniknąć moich roszczeń z tytułu utraty zdrowia. Według wojskowych przepisów, gdybym został zwolniony z wojska z powodów zdrowotnych, państwo musiałoby ponosić koszty wszystkich zabiegów i terapii związanych z odniesionym podczas szkolenia urazem. Administracyjne zwolnienie ze służby przerzucało wszystkie ewentualne koszty leczenia na mnie. Aby odzyskać wolność, musiałem się na to zgodzić.

Podpisałem oświadczenie i jeszcze tego samego dnia opuściłem szpital, podpierając się kulami, które amerykańska armia łaskawie pozwoliła mi

zatrzymać.

---

* 18 X-Ray – dosłownie: Prześwietlenie 18. W stosowanym w amerykańskiej armii systemie funkcji i specjalności (tzw. MOS, Military Occupational Specialty), liczba 18 stanowi przedrostek kodowych nazw funkcji pełnionych przez żołnierzy Sił Specjalnych – przykładowo 18 Bravo to specjalista ds. uzbrojenia, 18 Echo to specjalista ds. łączności, itp. (przyp. tłum.).

10_Upoważniony_i_zakochany|

Nie pamiętam, kiedy dokładnie w trakcie rekonwalescencji zacząłem na powrót trzeźwo myśleć. Najpierw musiał ustąpić ból, potem stopniowo ustąpiła również depresja, aż wreszcie, po tygodniach budzenia się bez żadnego celu poza śledzeniem upływu czasu na zegarku, powoli zaczęło do mnie docierać to, co mówili mi wszyscy wokół: wciąż jestem młody i przyszłość przede mną. W pełni uwierzyłem w to jednak dopiero wtedy, gdy mogłem stanąć prosto i przejść się o własnych siłach, co, jak się okazało, było jedną z tysięcy rzeczy, których wcześniej nie doceniałem – podobnie jak miłości rodziny.

Podczas pierwszych wypadów na teren ogrodu przed blokiem mamy zdałem sobie sprawę, że nie doceniałem czegoś jeszcze: łatwości, z jaką pojmowałem technologię.

Wybacz, jeśli zabrzmię jak nadęty dupek, ale nie da się tego inaczej ująć: całe życie czułem się tak swobodnie przy komputerze, że nie traktowałem swoich zdolności poważnie i nie chciałem zbierać za nie pochwał ani odnosić dzięki nim sukcesów. Przeciwnie, zależało mi, by ludzie doceniali mnie za coś innego – coś, co przychodziło mi z większym trudem. Chciałem pokazać, że nie jestem wyłącznie mózgiem w naczyniu, ale że mam również serce i mięśnie.

To dlatego zaciągnąłem się do wojska. Podczas rekonwalescencji zdałem sobie jednak sprawę, że choć to doświadczenie ubodło moją dumę, dodało mi też pewności siebie. Byłem teraz silniejszy, a ból nie budził we mnie strachu, tylko wdzięczność za to, jak pozytywnie na mnie wpłynął.

Życie za ogrodzeniem z drutu kolczastego stawało się coraz łatwiejsze. W ostatecznym rozrachunku przygoda z wojskiem kosztowała mnie tylko włosy, które zdążyły w międzyczasie odrosnąć, i nogi, których sprawność powoli wracała do normy.

Byłem gotów stawić czoła faktom: jeśli nadal pragnąłem służyć krajowi, a zdecydowanie tak było, musiałem działać, wykorzystując głowę i dłonie – za pośrednictwem komputera. Tylko tak mogłem dać z siebie to, co najlepsze. Choć weteran był ze mnie marny, fakt, że wojsko potwierdziło moją zdolność do służby, znacząco zwiększał moje szanse zdobycia pracy w jednej z agencji wywiadowczych; tam mój talent mógł przydać się najbardziej i tam być może czekały na mnie największe wyzwania.

Decyzja o pracy w wywiadzie oznaczała również i to, że pogodziłem się z czymś – patrząc z dzisiejszej perspektywy – nieuniknionym: potrzebą zdobycia poświadczenia bezpieczeństwa. W Stanach Zjednoczonych funkcjonują zasadniczo trzy poziomy niejawności informacji. I tak, poczynając od najniższego, są to: Confidential (poufne), Secret (tajne) i Top Secret (ściśle tajne). Ten ostatni może być rozszerzony o kwalifikator „szczególnie wrażliwe”, i tego właśnie poziomu uprawnienia do dostępu, oznaczanego akronimem TS/SCI (Top Secret / Sensitive Compartmented Information), wymagają stanowiska w najbardziej poważanych agencjach, czyli CIA i NSA. Jest on zdecydowanie najtrudniejszy do zdobycia i wymaga poddania się poszerzonemu, wyczerpującemu postępowaniu sprawdzającemu o nazwie Single Scope Background Investigation, ale otwiera wiele drzwi; wróciłem więc na Anne Arundel Community College, szukając równolegle jakiegoś zajęcia, które pozwoliłoby mi opłacić moją kandydaturę. Swoją drogą, bardzo polecam zdobywanie poświadczenia bezpieczeństwa kategorii TS/SCI każdemu, kto musi dojść do siebie po poważnym urazie, ponieważ proces przyznawania tych uprawnień może

zająć ponad rok. Wymaga wyłącznie uzupełnienia pewnej ilości dokumentacji; następnie można ułożyć się z wygodnie wyciągniętymi nogami i pilnować się, żeby nie popełnić zbyt wielu przestępstw, zanim rząd federalny wyda werdykt. Na resztę bowiem nie ma się wpływu.

W teorii byłem idealnym kandydatem. Pochodziłem z wojskowej rodziny, w której prawie każdy dorosły posiadał pewien poziom poświadczenia bezpieczeństwa. Zaciągnąłem się do wojska i próbowałem walczyć za ojczyznę, póki nie podciął mi skrzydeł nieszczęśliwy wypadek. Nie byłem uprzednio karany ani uzależniony od narkotyków. Jedyny dług, który posiadałem, stanowiła pożyczka studencka zaciągnięta w celu uzyskania certyfikatu Microsoftu; jej raty dotychczas zawsze spłacałem w terminie.

Mimo to nie potrafiłem się nie denerwować.

Jeździłem do college'u na zajęcia, a organizacja odpowiedzialna za moje postępowanie sprawdzające, nosząca nazwę National Background Investigation Bureau, wywracała do góry nogami niemal wszystkie aspekty mojego życia i przesłuchiwała prawie każdą osobę, którą znałem: moich rodziców, krewnych, kolegów z klasy, przyjaciół i znajomych. Audytorzy przeanalizowali moje nierówne wyniki w nauce i – jestem pewien – zasięgnęli języka wśród moich nauczycieli. Odniosłem wrażenie, że przepytali nawet Mae i Norma – oraz gościa, z którym pracowałem pewnego lata na stoisku z lodami w Six Flags America. Celem tego dochodzenia było nie tylko wykazanie, gdzie dałem plamę, ale i przekonanie się, na jaką manipulację i szantaż mogę być podatny. Z perspektywy służb wywiadowczych nie ma znaczenia, że nie jest się w stu procentach czystym, ponieważ wtedy przez sito nie przeszedłby ani jeden kandydat. Zależy im raczej, by sprawdzić, czy jesteś krystalicznie uczciwy – aby wywiad miał pewność, że nie ukrywasz żadnej mrocznej

tajemnicy, która mogłaby zostać wykorzystana przez jakąś wrogą siłę przeciw tobie, a tym samym przeciw agencji.

Uświadomienie sobie tego sprawiło, że zacząłem rozmyślać – kiedy stałem w korku, przez moją głowę przewijały się migawki wszystkich chwil, których w życiu żałowałem. Nic z tego, co sobie przypomniałem, nie wywołałoby, rzecz jasna, choćby drgnięcia brwi u śledczych, nawykłych do odkryć pokroju tego, że pewien czterdziestoletni analityk z think tanku ma upodobania do pieluch i biczowania przez babcie w skórzanych kostiumach. Cały proces wywoływał jednak pewną paranoję. Nie musisz być w tajemnicy fetyszystą, by mieć na koncie pewne wstydliwe zachowania i niepokoić się, że kiedy wyjdą na jaw, obce osoby mogą je opacznie zinterpretować. Mam na myśli, że – na miłość boską! – dorastałem przecież w internecie. Jeśli nie wpisałeś nigdy w pasku wyszukiwarki niczego gorszącego ani obrzydliwego, to znak, że korzystasz z sieci od bardzo niedawna. Pornografią się jednak nie przejmowałem. Porno oglądają wszyscy, a ci spośród was, którzy właśnie kręcą przecząco głowami, mogą się uspokoić: obiecuję, że nie zdradzę waszej tajemnicy. Mój niepokój brał się skądinąd – w każdym razie tak mi się wydawało. Chodziło o coś bardziej osobistego: o nieskończoną rzekę szowinistycznych głupot, jakie wypisywałem dojrzewając online, i jeszcze głupszych mizantropijnych opinii, choć tymczasem zdążyłem je już porzucić. Konkretnie: obawiałem się treści moich czatów internetowych i postów na forach, a także potencjalnych skutków absolutnie kretyńskich komentarzy, którymi upstrzyłem dziesiątki portali poświęconych grom i hakowaniu. Pod pseudonimem pisze się bez hamulców, często bezrefleksyjnie. A ponieważ współzawodnictwo o to, kto podzieli się czymś najbardziej prowokującym, stanowiło ważny element kultury wczesnego internetu, bez skrupułów zachęcałem na przykład do bombardowania państw, które opodatkowywały

gry komputerowe, albo wysyłania nieprzepadających za anime osób na przymusową reedukację w obozach. Nikt na rzeczonych portalach nie traktował tego poważnie, a już na pewno nie ja.

Kiedy czytałem ponownie swoje stare posty, krzywiłem się z zażenowania. Połowy tych rzeczy w ogóle nie miałem na myśli – chciałem po prostu być w centrum uwagi – ale słabo widziałem swoje szanse, gdyby przyszło mi tłumaczyć się z tego wszystkiego przed siwym mężczyzną w okularach w rogowych oprawkach, przeglądającemu gigantyczną kartotekę opatrzoną moim nazwiskiem. Druga połowa moich wpisów – kwestie, które faktycznie miałem na myśli – była jeszcze gorsza, bo pisząc ją, nie byłem już tamtym nieodpowiedzialnym dzieciakiem. Dorosłem. Na dodatek nie tylko nie uważałem tamtego głosu za własny, ale teraz czynnie przeciwstawiałem się wyrażanym wówczas opiniom – rozhisteryzowanym i dyktowanym przez hormony. Chciałem kłócić się z duchem. Walczyć z tą tępą, infantylną i bezmyślnie okrutną wersją siebie, która już nie istniała. Nie mogłem znieść myśli, że będzie mnie ona prześladować do końca życia, ale nie wiedziałem również, jak najlepiej wyrazić swój żal i się zdystansować, ani czy w ogóle powinienem to robić. Uważałem to za okrutne, że technologia nierozerwalnie związała mnie z przeszłością, której stuprocentowo żałowałem, choć ledwo ją przecież pamiętałem.

To może być chyba najbardziej powszechny problem osób z mojego pokolenia, pierwszego dorastającego z internetem w tle. Mogliśmy odkrywać i eksplorować swoje tożsamości prawie zupełnie bez nadzoru, nie myśląc w ogóle o tym, że nasze impulsywne wypowiedzi i wulgarne rozmowy są zapisywane na wieczność, a pewnego dnia możemy zostać pociągnięci za nie do odpowiedzialności. Jestem przekonany, że ci, którzy zaczęli korzystać z połączenia z internetem wcześniej, niż zdobyli pierwszą

pracę, zrozumieją, o co mi chodzi; z pewnością każda z takich osób ma w swojej historii jakiś wstydliwy wpis na forum, SMS bądź e-mail, które mogłaby przypłacić zwolnieniem.

Moja sytuacja przedstawiała się nieco inaczej: większość forów odwiedzanych przeze mnie w młodości pozwalała użytkownikom usuwać stare posty. Mogłem przygotować króciutki skrypt – nawet nie byłby on pełnowartościowym programem – i wszystkie moje wpisy ulotniłyby się w niecałą godzinę. Nie sprawiłoby mi to najmniejszej trudności. Wierz mi, brałem to pod uwagę.

Ostatecznie jednak nie potrafiłem się do tego przemóc. Coś mnie powstrzymywało. Miałem wrażenie, że zrobiłbym coś złego. Usuwając swoje posty raz na zawsze, nie złamałbym żadnego prawa ani nie uniemożliwił sobie uzyskania poświadczenia bezpieczeństwa, gdyby ktoś to odkrył. Mimo to dręczyło mnie przeświadczenie, że nie jest to dobry pomysł. Postępując w ten sposób, potwierdziłbym prawdziwość jednego z najbardziej toksycznych założeń internetowej rzeczywistości: że nikomu nie wolno popełnić ani jednego błędu, a każdy, kto sobie na to pozwoli, musi płacić za to do końca życia. Moim celem było więc w mniejszym stopniu zachowanie nienaruszonych pisemnych dowodów mojej działalności, a w większym – ochrona mojej duszy. Nie chciałem żyć w świecie, w którym wszyscy muszą udawać, że są idealni – nie było w nim miejsca ani dla mnie, ani dla moich przyjaciół. Usuwając swoje wpisy, wymazałbym to, kim byłem, jakie miałem korzenie i jak długą drogę przeszedłem. Zaprzeczając istnieniu mojego młodszego ja, zanegowałbym wartość osoby, którą się stałem.

Postanowiłem więc nie kasować starych wpisów i nauczyć się z nimi żyć. Doszedłem nawet do wniosku, że pełne oddanie tej postawie wymagało, bym nadal udzielał się na forach. W miarę upływu czasu

wyrosłem również z opinii z tamtego okresu, ale przekonania, które mną powodowało, trzymam się niezłomnie do dziś, choć chyba wyłącznie dlatego, że było ważnym krokiem na mojej drodze do dojrzałości. Nie sposób wymazać z internetu śladów będących dla nas źródłem wstydu i usunąć wpisów, w których się ośmieszyliśmy. Jedyne, co możemy kontrolować, to nasze reakcje: czy pozwolimy przytłoczyć się przeszłości, czy raczej wyciągniemy wnioski z odebranych lekcji, dojrzejemy i zostawimy to, co było, za sobą.

W tym mało dla mnie produktywnym, ale mocno formującym okresie, przyszło mi do głowy kilka przemyśleń; mógłbym je nazwać swoimi osobistymi zasadami. Ta wspomniana wcześniej była pierwszą. I choć nastręczyła mi kłopotów, do teraz staram się jej przestrzegać.

Być może zabrzmi to mało wiarygodnie, ale jedynymi śladami mojej minionej internetowej egzystencji, które nigdy nie wzbudziły we mnie uczucia gorszego niż lekkie zażenowanie, były moje profile na portalach randkowych. Podejrzewam, że to dlatego, iż musiałem je zakładać ze świadomością, że słowa, jakich użyję, powinny naprawdę coś znaczyć – wszak jedynym celem tego przedsięwzięcia było zainteresować kogoś ze świata rzeczywistego tym, co napisałem, a co za tym idzie: mną.

Zarejestrowałem się na założonym w 2000 roku portalu HotOrNot.com, najpopularniejszym z ówczesnych serwisów pozwalających oceniać zdjęcia. (W Stanach działały jeszcze między innymi RateMyFace i AmIHot. Młody Mark Zuckerberg połączył ich najbardziej udane funkcjonalności we własnym portalu, FaceMash, a ten później przeistoczył się w Facebooka). Popularność HotOrNot wynikała z prostego powodu: był najlepszy spośród tych nielicznych przedfacebookowych serwisów umożliwiających randkowanie.

Użytkownicy HotOrNot oceniali nawzajem swoje zdjęcia pod względem atrakcyjności i wydawali werdykt: „Hot” albo „Not”. Dodatkową funkcją, dostępną wyłącznie dla zarejestrowanych (w tym mnie), była możliwość kontaktowania się z innymi zarejestrowanymi, jeśli obie strony uważały swoje zdjęcia za atrakcyjne i kliknęły przycisk „Poznaj mnie”. Za pośrednictwem tego banalnego, prostackiego wręcz systemu poznałem moją partnerkę i miłość życia, Lindsay Mills.

Dziś oglądam tamte zdjęcia z rozbawieniem. Dziewiętnastoletnia Lindsay wyglądała na niezdarną, skrępowaną i urzekająco nieśmiałą. Ja jednak widziałem w niej powalająco piękną, absolutnie bombową blondynkę. Co więcej, jej fotografie same w sobie były piękne: cechował je wyraźny artyzm, miały więcej z autoportretów niż z selfie. Przyciągały wzrok i nie pozwalały go od siebie oderwać. W wyrafinowany sposób bawiły się światłem i cieniem. Niektóre zawierały nawet subtelne mrugnięcie okiem do oglądającego: jedno było zrobione w fotolabie, gdzie pracowała, a na innym Lindsay nie stała nawet przodem do obiektywu.

Przyznałem jej dziesięć punktów na dziesięć. Ku mojemu zaskoczeniu Lindsay też oceniła mnie pozytywnie (dała mi osiem punktów, kochana) i chwilę później już czatowaliśmy. Okazało się, że Lindsay studiuje profesjonalną fotografię artystyczną. Miała własną stronę internetową, na niej prowadziła pamiętnik i zamieszczała zdjęcia lasów, kwiatów, opuszczonych fabryk i – te ostatnie podobały mi się najbardziej – siebie samej.

Przeczesałem internet i utworzyłem w myślach pełniejszy obraz Lindsay, wykorzystując wszystkie informacje, które znalazłem na jej temat: miejscowość, gdzie się urodziła (Laurel w stanie Maryland), nazwę jej uczelni (MICA, czyli Maryland Institute College of Art). Przedzierzgnąłem się w sieciowego stalkera, do czego się później przyznałem. Czułem się

z tym obrzydliwie, ale Lindsay nie chciała słuchać, jak się nad sobą użalam. „Ja też szukałam informacji o tobie, mądralo” – skwitowała sprawę i wklepała w okienko czatu cała listę faktów na mój temat.

Były to jedne z najmilszych słów, jakie w życiu słyszałem, ale wciąż wzdragałem się przed spotkaniem twarzą w twarz. Umówiliśmy się na randkę i w miarę upływu dni, które do niej pozostały, robiłem się coraz bardziej nerwowy. Przeniesienie internetowej znajomości do realu to przerażająca propozycja. Bałbym się nawet w świecie, gdzie nie istnieją oszuści ani mordercy goniący ludzi z siekierą, bo z doświadczenia wiedziałem, że im intensywniej kontaktowało się z kimś przez internet, tym większy zawód przeżywało się, poznając tego kogoś na żywo. Tematy, jakie bez trudu porusza się na ekranie, nie chcą przejść przez usta w rozmowie w cztery oczy. Dystans sprzyja zażyłości: nikt nie rozmawia szczerzej niż dwie osoby, które nie widzą się nawzajem, zamknięte we własnych pokojach. Kiedy jednak spotkasz się ze swoim rozmówcą, wrażenie swobody znika. Zaczynasz wypowiadać się w bezpieczniejszy, bardziej utemperowany sposób, jak w każdej zwykłej rozmowie na neutralnym gruncie.

W sieci powierzaliśmy sobie wszystkie tajemnice i bałem się, że kiedy spotkam się z Lindsay osobiście, stracę tę więź. Innymi słowy, bałem się odrzucenia.

Niepotrzebnie.

Umówiliśmy się z Lindsay – uparła się, że po mnie przyjedzie – pod blokiem mojej mamy. O umówionej godzinie stałem na zewnątrz w wieczornym chłodzie i z telefonem przy uchu starałem się pokierować ją przez gąszcz identycznie wyglądających i podobnie nazwanych osiedlowych ulic. Wypatrywałem złotego chevroleta cavalier rocznik 98, gdy nagle oślepił mnie padający prosto na moją twarz strumień światła

z krawężnika. To Lindsay błyskała do mnie długimi światłami, a ich blask odbijał się od śniegu.

– Zapnij się – brzmiały pierwsze słowa, które usłyszałem z jej ust, kiedy tylko wsiadłem do samochodu. W następnym zdaniu zapytała: – To jaki mamy plan?

W tej samej chwili zdałem sobie sprawę, że choć spędziłem mnóstwo czasu, rozmyślając o niej, nie poświęciłem ani chwili rozważaniom na temat tego, gdzie się udamy.

Gdybym znalazł się w tej sytuacji z jakąkolwiek inną kobietą, zacząłbym improwizować, udawać, że coś zaplanowałem. Przy Lindsay nie odczuwałem jednak takiej potrzeby. W jej towarzystwie to było bez znaczenia. Pojechaliśmy jej ulubioną ulicą – miała swoją ulubioną ulicę! – i rozmawialiśmy, aż dotarliśmy do końca ciągnącej się przez wiele mil Guilford, po czym zatrzymaliśmy się na parkingu przy centrum handlowym Laurel i po prostu siedzieliśmy w samochodzie, wciąż rozmawiając.

Było idealnie. Rozmowa twarzą w twarz okazała się najzwyklejszą kontynuacją wszystkich naszych rozmów telefonicznych, e-maili i czatów internetowych. Pierwsza randka była ciągiem dalszym naszego pierwszego kontaktu online i punktem wyjściowym konwersacji, która będzie trwała tak długo, jak długo będziemy żyli. Rozmawialiśmy o naszych rodzinach, a raczej o tym, co z nich zostało. Rodzice Lindsay też byli rozwiedzeni: jej matka i ojciec mieszkali w odległości dwudziestu minut jazdy samochodem i jako dziecko była nieustannie wożona pomiędzy jednym a drugim domem. Cały swój dobytek woziła w torbie. W poniedziałki, środy i piątki spała w swoim pokoju w domu mamy. We wtorki, czwartki i soboty – w swoim pokoju w domu ojca. Niedziela zaś była dniem rozdarcia – musiała wybierać.

Powiedziała mi, jak okropny mam jej zdaniem gust, i skrytykowała mój ubiór, który wybrałem na randkę: dżinsy i narzuconą na podkoszulek koszulę z kołnierzykiem na guziki, ozdobioną metalicznym motywem płomieni. (Przepraszam). Opowiedziała mi o dwóch innych chłopakach, z którymi się spotykała, o czym zresztą wspominała mi wcześniej w sieci. Sam Machiavelli nabrałby rumieńców z podekscytowania, gdyby odkrył, do jakich sposobów się uciekłem, by podkopać ich szanse. (Nie przepraszam). Sam też opowiedziałem jej wszystko o sobie, przyznając się między innymi, że nie będę mógł z nią rozmawiać o swojej pracy – o tej, której jeszcze nie podjąłem. Sposób, w jaki to mówiłem, był absurdalnie pretensjonalny, co Lindsay dała mi jasno do zrozumienia, kiwając głową z wielką powagą.

Wyjaśniłem, że niepokoję się nadchodzącym badaniem wariograficznym wymaganym do zdobycia potwierdzenia bezpieczeństwa. Lindsay zaproponowała, że ze mną poćwiczy. Taka głupkowata gra wstępna. Filozofia, którą wyznawała, zapewniała idealny trening: mów, co chcesz, mów, kim jesteś, niczego się nie wstydź. Jeśli cię odrzucą, to ich problem. Jeszcze nigdy nie czułem się przy drugiej osobie tak swobodnie i jeszcze nigdy tak bardzo nie przeszkadzało mi to, że ktoś wytyka moje wady. Pozwoliłem nawet, żeby zrobiła mi zdjęcie.

Głos Lindsay rozbrzmiewał w mojej głowie, kiedy jechałem w stronę kompleksu NSA o dziwacznej nazwie Friendship Annex (Aneks Przyjaźni), by odbyć ostatnie przesłuchanie wymagane w procesie przyznawania dostępu do informacji niejawnych. Znalazłem się w pokoju bez okien, przywiązany niczym zakładnik do taniego krzesła biurowego. Moją klatkę piersiową i brzuch oplatały rurki pneumografu – aparatu rejestrującego oddech. Klipsy założone na opuszki palców miały badać moją reakcję skórno-galwaniczną, opaska na ramieniu – ciśnienie krwi i tętno,

a podkładka sensoryczna na siedzeniu krzesła – najdrobniejsze ruchy i zmiany pozycji. Cały ten sprzęt – przypięty, zatrzaśnięty, nałożony i przymocowany mocnymi pasami do mojego ciała – był połączony z dużym czarnym urządzeniem ustawionym przede mną na stole: wariografem.

Po drugiej stronie blatu, na wygodniejszym krześle, siedziała operatorka. Przypominała mi jedną z moich dawnych nauczycielek – dlatego też spędziłem większą część testu, usiłując przypomnieć sobie nazwisko tamtej kobiety albo próbując tego nie robić. W pewnej chwili zaczęła – wariografistka, nie nauczycielka – zadawać pytania. Początkowe były banalne. Czy nazywam się Edward Snowden? Czy moja data urodzenia to 21 czerwca 1983 roku? Później usłyszałem: czy popełniłem kiedykolwiek jakieś poważne przestępstwo? Czy borykałem się z uzależnieniem od hazardu? Czy byłem uzależniony od alkoholu albo stosowałem nielegalne substancje odurzające? Czy kiedykolwiek pracowałem jako agent obcego kraju? Czy kiedykolwiek opowiadałem się za obaleniem rządu Stanów Zjednoczonych na drodze przemocy? Wolno mi było udzielać wyłącznie binarnych odpowiedzi: „tak” lub „nie”. Na wiele pytań odpowiadałem „nie” i wyczekiwałem tych, których panicznie się bałem. Czy kiedykolwiek kwestionowałem w internecie kompetencje i etykę personelu medycznego bazy Fort Benning? Czego szukałem na serwerach ośrodka badań atomowych Los Alamos? Nie usłyszałem ich jednak i zanim się zorientowałem, test dobiegł końca.

Zdałem śpiewająco.

Zgodnie z wymogami musiałem odpowiedzieć na tę samą serię pytań trzy razy i za każdym razem przeszedłem test pomyślnie, co oznaczało, że zaliczyłem badanie poligrafem w najszerszym możliwym zakresie, a więc

mogłem otrzymać potwierdzenie bezpieczeństwa klasy TS/SCI – najwyższe dostępne w kraju.

Byłem zakochany z wzajemnością. Przez to wszystko czułem się jak w niebie.

Miałem dwadzieścia dwa lata.

Część_02|

11_System|

W tym miejscu włączę na chwilę pauzę, żeby coś wyjaśnić – chodzi o moje poglądy polityczne, jakie wyznawałem w wieku dwudziestu dwóch lat. Nie miałem żadnych. Zamiast nich, jak większość młodych ludzi, posiadałem niewzruszone przekonania, które tak naprawdę nie były moje, lecz stanowiły pełną sprzeczności zbitkę reguł odziedziczonych po innych. Moją głowę wypełniała mieszanina wartości, z którymi się wychowałem, i ideałów, którymi przesiąkłem w sieci. Dopiero zbliżając się do trzydziestych urodzin, zrozumiałem nareszcie, jak ogromna część tego, o czym byłem przekonany, a raczej: co uważałem za swoje przekonania, była po prostu poglądami wpojonymi mi za młodu. Uczymy się mówić, naśladując mowę dorosłych ze swojego otoczenia, i w trakcie tego procesu zaczynamy powielać również ich opinie, rojąc sobie, że jesteśmy autorami słów, którymi się posługujemy.

Moi rodzice mieli lekceważący stosunek może nie do polityki jako takiej, ale do samych polityków – to na pewno. Należy jednak podkreślić, że ich nastawienie miało niewiele wspólnego ze zniechęceniem charakterystycznym dla tych, co nie głosują, bądź pogardą dla konkretnej partii. Chodziło raczej o swego rodzaju bezstronność, typową dla ich klasy społecznej. Rodziców w szlachetniejszej epoce nazywano by urzędnikami federalnymi albo pracownikami sektora publicznego; w naszych czasach zaś mówi się o nich: państwo w państwie lub rząd cieni. Żadne z tych określeń nie oddaje jednak trafnie roli, jaką osoby z kręgu moich rodziców odgrywają jako zawodowi urzędnicy państwowi (i przy

okazji jako prawdopodobnie jedna z ostatnich normalnie funkcjonujących warstw amerykańskiej klasy średniej). Ci ludzie – choć nie dostali mandatu w wyborach ani nie otrzymali nominacji – służą rządowi w niezależnych agencjach (od CIA i NSA po urząd podatkowy, Federalną Komisję Łączności i tym podobne) albo w jednym z departamentów reprezentujących władzę wykonawczą (Departamencie Stanu, Skarbu, Obrony, Sprawiedliwości i tak dalej).

To właśnie było środowisko moich rodziców, grupa, z którą się identyfikowałem: licząca niemal trzy miliony osób profesjonalna siła robocza, wspierająca z oddaniem amatorów wybieranych przez elektorat i wybrańców nominowanych przez tychże amatorów w realizacji zadań politycznych, czy też – zgodnie ze słowami ślubowania – w sumiennym wykonywaniu obowiązków wobec narodu. Podczas gdy kolejne administracje przemijają, urzędnicy ci pozostają na stanowiskach, i pracują równie sumiennie pod przywództwem republikanów, co demokratów. Nie służą określonej partii, a samemu rządowi, zapewniając fundamentalną ciągłość i stabilność władzy.

Ludzie ci odpowiedzieli również na wezwanie kraju, kiedy ten zaangażował się w wojnę. Tak postąpiłem i ja po atakach na World Trade Center, odkrywając przy okazji, że patriotyzm, który wpoili mi rodzice, łatwo przeistaczał się w nacjonalistyczny ferwor. Przez pewien czas, szczególnie w okresie przed zaciągnięciem się do armii, mój obraz świata zaczął bardzo przybierać kształt dualizmu najmniej wyrafinowanych gier komputerowych, w których dobro i zło są jasno zdefiniowane i niepodważalnie odrębne.

Rzecz w tym, że kiedy wróciłem z wojska i na powrót zająłem się informatyką, stopniowo zacząłem żałować swoich militarnych fantazji. Im bardziej rozwijałem umiejętności, tym mocniej dojrzewałem i zdawałem

sobie sprawę, że technologia komunikacji ma szansę podołać tam, gdzie technologia przemocy zawiodła. Nie dało się narzucić ludziom demokracji, grożąc im bronią, ale możliwe, że udałoby się ją zasiać, rozszerzając zasięg naszej sieci krzemu i światłowodów. Na początku pierwszej dekady XXI wieku internet był wciąż w powijakach i – przynajmniej z mojego punktu widzenia – stanowił bardziej autentyczne i pełniejsze wcielenie amerykańskich ideałów niż sama Ameryka. Miejsce, gdzie wszyscy byli równi? Tak. Miejsce stworzone z myślą o życiu, wolności i pogoni za szczęściem? Tak, tak, tak. W dodatku niemal wszystkie dokumenty założycielskie kultury internetowej opisywały sieć językiem przywołującym na myśl historię Stanów Zjednoczonych: oto mieliśmy przed sobą wielki, nieujarzmiony Dziki Zachód należący do każdego, kto odważył się na nim osiedlić, zapełniający się jednak błyskawicznie koloniami finansowanymi przez rządy i korporacje, które dążyły do narzucenia przepisów zapewniających im władzę i zysk. Wielkie firmy żądały wysokich honorariów – za sprzęt, oprogramowanie, międzymiastowe połączenia telefoniczne, bo to one służyły w tamtych czasach do łączenia się z internetem, i za wiedzę samą w sobie – coś, co stanowi przecież wspólne dziedzictwo ludzkości i co powinno być dostępne za darmo dla wszystkich. Trudno było nie dostrzegać w tych instytucjach nowoczesnego wcielenia Imperium Brytyjskiego, którego okrutna polityka podatkowa obudziła w mieszkańcach kolonii pragnienie niepodległości.

Ta nowa rewolucja nie odbywała się na stronach podręczników do historii, lecz w czasach mojego pokolenia, i każdy z nas dzięki posiadaniu pewnych umiejętności mógł stać się jej częścią. To było ekscytujące – brać udział w zakładaniu nowego społeczeństwa, w którym nie liczyło się, gdzie się urodziłeś, w jakich warunkach dorastałeś ani czy byłeś lubiany w liceum, lecz to, jak duże posiadasz wiedzę i zdolności z zakresu

technologii. W szkole musiałem nauczyć się na pamięć preambuły konstytucji Stanów Zjednoczonych. Teraz jej słowa tkwiły w mojej pamięci obok artykułu Johna Perry'ego Barlowa zatytułowanego *Deklaracja niepodległości cyberprzestrzeni*, który – podobnie jak historyczna *Deklaracja niepodległości Stanów Zjednoczonych* – odwołuje się do pewnych oczywistych prawd i zwraca się do czytelnika w pierwszej osobie liczby mnogiej: „Tworzymy świat otwarty dla wszystkich, w którym każdemu przysługują te same prawa niezależnie od rasy, zamożności, potęgi wojskowej czy pochodzenia. Tworzymy świat, w którym każdemu wolno w dowolnym miejscu wyrażać swoje przekonania, nieważne jak osobliwe, bez lęku o to, że zostanie zmuszony do milczenia lub nakłoniony do konformizmu".

Udział w tej technologicznej merytokracji dawał silne poczucie panowania nad swoim losem, ale również uczył pokory, czego zasmakowałem, kiedy podjąłem pierwszą pracę w służbach wywiadowczych. Decentralizacja internetu wyłącznie podkreśliła znaczenie decentralizacji umiejętności komputerowych. Mogłem być najlepszym informatykiem w rodzinie lub w okolicy, ale praca dla wywiadu oznaczała konieczność mierzenia się z moimi odpowiednikami z całego kraju i świata. Internet pokazał mi, jak niesamowicie liczne i różnorodne są ludzkie talenty, i dał mi jasno do zrozumienia, że jeśli chcę coś osiągnąć, muszę zdobyć specjalizację.

Technologia komputerowa oferowała kilka rodzajów kariery. Mogłem zostać deweloperem oprogramowania, czyli popularnie zwanym programistą, i pisać kod, który sprawia, że komputery wykonują swoje zadania. Mogłem również wykształcić się na specjalistę do spraw sprzętu albo sieci i zająć się instalacją serwerów w szafach, prowadzeniem okablowania, pleceniem potężnej struktury spinającej wszystkie komputery,

urządzenia i pliki. Komputery wraz z oprogramowaniem zawsze mnie interesowały; łącząca sprzęt sieć również. Najbardziej jednak intrygowało mnie współdziałanie komputerów z siecią na wyższym poziomie abstrakcji: nie jako indywidualnych podzespołów, lecz wszechogarniającego systemu.

Wiele rozmyślałem na ten temat za kierownicą w drodze do domu Lindsay, na zajęcia w college'u i podczas powrotów. Od kiedy zacząłem prowadzić, wykorzystywałem godziny spędzane w samochodzie na przemyślenia, a dojazdy zatłoczoną obwodnicą zajmowały dużo czasu. Jako programista miałbym podobną rolę co osoba odpowiedzialna za prowadzenie miejsc obsługi podróżnych przy zjazdach z głównej drogi – dbałbym o taki układ franczyz restauracyjnych i stacji benzynowych, by zapewniał on zdrową konkurencję i zaspokajał potrzeby klientów. Jako specjalista do spraw sprzętowych musiałbym budować infrastrukturę oraz samodzielnie wytyczać i utwardzać drogi. Jako administrator sieci byłbym zaś odpowiedzialny za zarządzanie ruchem, ustawianie znaków i sygnalizatorów świetlnych w taki sposób, by bezpiecznie doprowadzać wiecznie spieszące się hordy do miejsc, do których zmierzają. Gdyby jednak udało mi się zostać osobą związaną z zarządzaniem systemami, pełniłbym rolę urbanisty: dbał o to, by wszystkie dostępne elementy współgrały ze sobą z jak najlepszym skutkiem. Była to praca, w której, mówiąc wprost, dostawało się pieniądze za zabawę w boga, a przynajmniej w podrzędnego dyktatora.

Zasadniczo istnieją dwa rodzaje stanowisk związanych z zarządzaniem systemem informatycznym. W pierwszym wypadku obejmuje się pieczę nad całym istniejącym już systemem i utrzymuje się go, stopniowo starając się poprawiać jego wydajność i naprawiając go, kiedy szwankuje. Stanowisko to nosi nazwę administratora systemu – sysadmina. Drugi rodzaj pracy z systemami polega na analizowaniu ich potrzeb związanych

na przykład z przechowywaniem danych albo z przeszukiwaniem kilku baz jednocześnie, a następnie na projektowaniu rozwiązań z wykorzystaniem istniejących już elementów bądź wymyślaniu zupełnie nowych. Osoby, które się tym zajmują, to inżynierowie systemów informatycznych. W swojej karierze miałem okazję pracować na obu tych stanowiskach – najpierw udało mi się zdobyć stanowisko administratora, a następnie zostałem inżynierem. Przez cały czas nie zdawałem sobie jednak sprawy, w jaki sposób takie intensywne zaangażowanie w pracę przy systemach komputerowych o najwyższym możliwym poziomie integracji wywiera wpływ na moje poglądy polityczne.

Postaram się, by moje wyjaśnienia nie były zbyt abstrakcyjne, ale chciałbym, żebyś wyobraził sobie jakiś system. Dowolny: ekosystem, system komputerowy, prawa, a nawet władzy. Pamiętaj, system to po prostu zestaw elementów funkcjonujących jako całość, o czym większość ludzi przypomina sobie dopiero wtedy, gdy coś się zepsuje. Jednym z najbardziej pouczających faktów dotyczących pracy z systemami jest to, że przestający prawidłowo funkcjonować komponent prawie nigdy nie jest tym, w którym zdiagnozowałeś awarię. Aby odkryć, co spowodowało zapaść systemu, musisz posłużyć się logiką i prześledzić ścieżkę problemu przez wszystkie części składowe, poczynając od miejsca, w którym został zauważony. Z racji tego, że naprawa takich usterek należy do obowiązków administratorów i inżynierów systemów, praca ta wymaga biegłości i w programowaniu, i w sprawach sprzętowych, i w zagadnieniach związanych z sieciami. Jeśli problem okaże się mieć podłoże programistyczne, naprawa może wymagać dokładnego – linia po linii – czytania kodu napisanego w liczbie języków programowania dorównującej liczbie krajów obecnych na Zgromadzeniu Ogólnym ONZ. Kiedy sprawa jest natury sprzętowej, konieczne może być sprawdzenie wszystkich

połączeń na konkretnej płytce drukowanej, z latarką w zębach i lutownicą w dłoni. Gdy z kolei poszlaki wskazują na awarię sieci, może to wymagać dokładnego sprawdzenia każdego z kabli plątaniny biegnącej w suficie i pod podłogą, która łączy odległe ośrodki danych pełne serwerów z biurami pełnymi laptopów.

Ponieważ systemy pracują w oparciu o instrukcje, czyli zasady, analiza potrzebna do naprawy jest w praktyce poszukiwaniem odpowiedzi na pytanie, które instrukcje, kiedy i w jaki sposób zawiodły. Ma to na celu ustalenie konkretnych okoliczności, w jakich określone sformułowanie zasady lub jej zastosowanie jest nieadekwatne do faktycznych intencji twórcy. Czy system uległ awarii, ponieważ nie przekazano pewnych informacji? Czy może dlatego, że ktoś dopuścił się naruszenia, zdobywając nieuprawniony dostęp do pewnego zasobu albo nadużywając dostępu, do którego miał uprawnienia? Czyżby któryś z podzespołów spowodował przerwanie albo utrudnienia pracy innego? A może jeden z programów lub komputerów, lub zespołów użytkowników wykorzystał więcej zasobów systemu, niż mu przysługiwało?

W miarę rozwoju mojej kariery coraz trudniej było mi zadawać tego rodzaju pytania tylko w odniesieniu do systemów informatycznych, za które odpowiadałem, a nie w stosunku do swojego kraju. Zdolność do naprawy tych pierwszych, ale nie tego drugiego, stała się dla mnie źródłem narastającej frustracji. Kończąc przygodę z wywiadem, byłem przekonany, że system operacyjny Stanów Zjednoczonych – czyli jego rząd – doszedł do wniosku, że najlepiej funkcjonuje w stanie awarii.

12_Homo_contractus

Miałem nadzieję służyć krajowi, tymczasem zostałem przez niego zatrudniony. Nie jest to błaha różnica. Podczas gdy ojciec i dziadek piastowali stanowiska gwarantujące swego rodzaju stabilność i poszanowanie, ja, podobnie jak większość osób z mojego pokolenia, nie mogłem liczyć na nic podobnego. Dla ojca i dziadka pierwszy dzień zawodowej służby był pierwszym dniem dorosłej pracy, a dzień, gdy odeszli na emeryturę – ostatnim. Tak działał rząd, który znałem od najwcześniejszego dzieciństwa – kiedy pomagał mnie wyżywić, ubrać i zapewnić dach nad głową – aż po dzień, gdy wydał mi poświadczenie bezpieczeństwa umożliwiające pracę w wywiadzie. Rząd ten traktował służbę obywatela jako nienaruszalny układ: w zamian za lojalność i poświęcenie krajowi najproduktywniejszych lat życia obiecywał zadbać o ciebie i twoją rodzinę.

Okres, kiedy rozpocząłem pracę w wywiadzie, należał już do innej ery.

Zanim objąłem moje pierwsze stanowisko, szczerość służby publicznej zdążyła ustąpić miejsca zachłanności sektora prywatnego, a uświęcony pakt pomiędzy żołnierzami, oficerami i zawodowymi urzędnikami coraz częściej zastępowały ponure układy z *Homo contractus*, dominującym gatunkiem rządu amerykańskiego w wersji 2.0. Kreatura ta nie była zaprzysiężonym urzędnikiem, lecz migrantem zarobkowym, czyjego patriotyzm wspomagano podwyżkami pensji i który nie postrzegał rządu federalnego jako najwyższego zwierzchnika, lecz najważniejszego klienta.

Podczas wojny o niepodległość Stanów Zjednoczonych decyzja Kongresu Kontynentalnego o zatrudnianiu korsarzy i najemników do obrony ledwie funkcjonującej republiki miała sens. W przypadku Ameryki z pierwszych lat trzeciego tysiąclecia naszej ery, państwa o statusie hipermocarstwa, wydało mi się jednak dziwaczne i poniekąd złowieszcze, by powierzać obronność narodową siłom prywatnym. Słusznie zresztą, bo dziś praca kontraktowa dla rządu kojarzy się przede wszystkim z najgłośniejszymi skandalami, na przykład sprawą najemników z korporacji Blackwater (zmieniła nazwę na Xe Services po tym, jak jej pracownicy zostali uznani winnymi zabójstwa czternastu irackich cywilów, a później na Academi, kiedy przejęła ją grupa prywatnych inwestorów) albo oprawców z firm CACI i Titan (zapewniły personel odpowiedzialny za terroryzowanie więźniów w Abu Ghurajb).

W opinii publicznej te sensacyjne przypadki mogą stanowić sugestię, że rząd zleca prywatnym podmiotom zadania, które są nielegalne bądź należą do szarej strefy, by w razie potrzeby móc wyprzeć się odpowiedzialności i zachować czyste ręce oraz sumienie. Nie jest to jednak do końca prawda, a w każdym razie nie w kontekście pracy sił wywiadowczych. Wywiadowi bowiem zależy nie tyle na możliwości wyparcia się swojego udziału, co na tym, by jego poczynania w ogóle nie zostały wykryte. Wykorzystuje pracowników kontraktowych w dużo bardziej przyziemnym celu. Mianowicie umożliwiają oni jego agencjom obejście – można by rzec: zhakowanie – federalnych limitów zatrudnienia. Wszystkie agencje obowiązują bowiem ustawowo narzucone ograniczenia liczby osób, która może zostać zatrudniona do wykonywania poszczególnych kategorii zadań. Pracownicy kontraktowi tymczasem – z racji tego, że nie są bezpośrednio zatrudnieni przez rząd federalny – nie wliczają się w poczet tych limitów. Agencje mogą zatrudnić taką ich liczbę, na jaką je stać, a stać je na

dowolną – wystarczy, że udadzą się na żebry do Kongresu i zeznają przed kilkoma wybranymi podkomisjami, że terroryści czają się na nasze dzieci, Rosjanie siedzą w naszej poczcie elektronicznej, a Chińczycy – w naszej sieci energetycznej. Argumenty te w gruncie rzeczy stanowią zawoalowane groźby, a Kongres konsekwentnie im ulega i przystaje na wszystkie żądania.

Wśród dokumentów, które przekazałem dziennikarzom, znajdował się Czarny Budżet na rok 2013 – tajny plan wydatków na 52,6 miliarda dolarów; sumę tę zarezerwowano w ponad sześćdziesięciu ośmiu procentach na potrzeby sił wywiadowczych, między innymi na wypłacenie pensji 107 035 osobom, w tym 21 800 pełnoetatowym pracownikom kontraktowym. Liczba ta, choć ogromna, nie obejmowała dziesiątek tysięcy personelu zatrudnianych przez firmy, które podpisały kontrakty (albo podkontrakty, albo podpodkontrakty) z agencjami wywiadu na wykonanie różnych usług i przedsięwzięć. Rząd nigdy nie uwzględnia pracowników tego rodzaju w swoich obliczeniach, nawet na potrzeby Czarnego Budżetu, ponieważ oficjalne wliczenie ich w poczet pracowników kontraktowych z absolutną jasnością unaoczniłoby niepokojący fakt: praca amerykańskiego wywiadu jest wykonywana w tym samym stopniu przez osoby prywatne, co przez funkcjonariuszy rządowych.

Oczywiście wiele osób, nawet należących do rządu, utrzymuje, że układ ten ma wiele zalet. Kontrakty ich zdaniem zachęcają przedsiębiorstwa do konkurencji w przetargach i zwalniają rząd z obowiązku wypłacania emerytur oraz świadczeń. Największą zaletą z perspektywy urzędników rządowych jest jednak konflikt interesów nieodłącznie związany z procesem planowania wydatków. Dyrektorzy agencji wywiadowczych proszą Kongres o pieniądze na wynajęcie pracowników kontraktowych od prywatnych firm, członkowie Kongresu zatwierdzają te środki, po czym

i dyrektorzy, i kongresmeni biorący udział w przedsięwzięciu są nagradzani po odejściu ze stanowiska wysokopłatnymi etatami bądź stanowiskami konsultantów w firmach, które wzbogaciły się dzięki ich decyzjom. Z perspektywy korporacyjnych zarządów kontrakty są formą rządowo wspomaganej korupcji – najbardziej legalną i najwygodniejszą ze wszystkich funkcjonujących w Ameryce metod przekazywania publicznych środków do prywatnych kieszeni.

Co więcej, mimo daleko posuniętej prywatyzacji wywiadu jedyną instytucją, która przyznaje poświadczenia bezpieczeństwa umożliwiające dostęp do informacji niejawnych, pozostaje rząd federalny. A z racji tego, że każda osoba aplikująca o poświadczenie musi posiadać sponsora – co oznacza, że musi zdobyć propozycję pracy na stanowisku wymagającym dostępu do poufnych danych – większość pracowników kontraktowych rozpoczyna karierę na stanowisku rządowym. Prywatnej firmie rzadko opłaca się ufundować pracownikowi aplikację, a następnie wypłacać mu pensję za czekanie, potencjalnie ponad rok, aż rząd przyzna mu uprawnienia. Pod względem finansowym dużo sensowniejszym posunięciem jest zatrudnić osobę, która otrzymała już poświadczenie bezpieczeństwa. Podejście to doprowadziło do sytuacji, kiedy rząd ponosi całkowity ciężar wydawania poświadczeń, ale niewiele zyskuje w zamian. Bierze na siebie całą pracę i wszelkie koszty związane z audytem kandydata, a ten w wielu wypadkach z chwilą otrzymania poświadczenia rzuca się do drzwi, żeby wymienić niebieski identyfikator pracownika rządowego na zielony pracownika kontraktowego. Popularny żart głosi, że zieleń plakietki symbolizuje pieniądze.

Rządowe stanowisko, dzięki któremu mogłem ubiegać się o poświadczenie bezpieczeństwa kategorii TS/SCI, nie spełniało moich oczekiwań, ale tylko takie udało mi się znaleźć: byłem oficjalnie

zatrudniony przez stan Maryland i pracowałem dla Uniwersytetu Stanowego Maryland w College Park. Uczelnia pomagała NSA otworzyć nową instytucję – Center for Advanced Study of Language (CASL, Ośrodek Zaawansowanych Badań Językowych).

Oficjalnie misją ośrodka było badanie, w jaki sposób ludzie uczą się języków, i opracowywanie wspieranych komputerowo metod nauki, które pozwalałyby przyswajać materiał szybciej i skuteczniej. Drugie dno polegało na tym, że NSA zależało na opracowaniu technologii umożliwiających komputerom lepsze rozumienie języka. Podczas gdy inne agencje miały w tym czasie kłopot ze znalezieniem kompetentnych osób posługujących się językiem arabskim (a także perskim, dari, paszto i kurdyjskim), do tego spełniających ich czasami absurdalne wymogi bezpieczeństwa (na przykład nieposiadających nawet daleko spokrewnionego niewygodnego kuzyna) i mogących wykonywać pracę tłumaczy pisemnych i ustnych w terenie, NSA borykała się z innym problemem: ponieważ przechwytywała ogromne ilości przekazów w obcych językach, odczuwała palącą potrzebę zapewnienia swoim komputerom zdolności ich rozumienia i analizowania.

Nie mam dokładniejszego pojęcia, jakimi projektami miał się zajmować CASL, z tego prostego powodu, że kiedy stawiłem się do pracy, uzbrojony w moje świeżutkie poświadczenie bezpieczeństwa, ośrodek nie był jeszcze otwarty. Budynek dopiero powstawał. Póki nie został wykończony i nie zainstalowano w nim potrzebnego sprzętu, pełniłem zasadniczo rolę nocnego stróża. Moje obowiązki ograniczały się do codziennego pojawiania się na miejscu, patrolowania pustych korytarzy po wyjściu pracowników budowlanych – również kontraktowych – i pilnowania, by nikt nie podłożył ognia ani nie włamał się i nie zamontował podsłuchu. Spędziłem niezliczone godziny, krążąc po częściowo wykończonym obiekcie

i przyglądając się postępom dokonanym minionego dnia: a to usiadłem na próbę w jednym z foteli świeżo zainstalowanych w supernowoczesnej auli, a to rzucałem kamieniami po dachu wyłożonym pod moją nieobecność otoczakami; podziwiałem też nowe ściany z płyty gipsowo-kartonowej i dosłownie przyglądałem się, jak schnie farba.

Tak wygląda życie ochroniarza pilnującego ściśle tajnego obiektu po godzinach normalnej pracy i – szczerze mówiąc – nie przeszkadzało mi to. Płacono mi zasadniczo za nic, musiałem tylko krążyć w ciemności w towarzystwie własnych myśli, a brak obowiązków sprawiał, że miałem tyle czasu, ile tylko chciałem, by na jedynym działającym komputerze, do którego miałem dostęp, szukać nowej pracy. Za dnia nadrabiałem sen i jeździłem na wyprawy fotograficzne z Lindsay, która – na skutek moich zalotów i niecnych machinacji – rzuciła nareszcie pozostałych chłopaków.

W tamtym okresie byłem jeszcze dostatecznie naiwny, by roić sobie, że praca w CASL-u posłuży mi za pomost do pełnoprawnej kariery w rządzie federalnym. Im dłużej jednak rozglądałem się po rynku pracy, tym bardziej zaskakiwało mnie, jak niewiele istniało okazji, by bezpośrednio służyć krajowi – w każdym razie na nietrywialnym stanowisku technicznym. Dużo lepsze szanse na zatrudnienie miałem jako pracownik kontraktowy w prywatnej firmie służącej państwu za pieniądze. Najlepsze zaś możliwości, okazało się, dawała mi praca podwykonawcy prywatnej firmy będącej podwykonawcą innej prywatnej firmy, która służyła mojemu krajowi za pieniądze. Kiedy zdałem sobie z tego sprawę, doznałem szoku.

Szczególnie absurdalne wydało mi się to, że sprywatyzowana była większość stanowisk administracyjnych związanych z projektowaniem i administracją systemów informatycznych – stanowisk wymagających przecież niemal pełnego dostępu do cyfrowej egzystencji pracodawcy. W wypadku dużego banku albo nawet firmy z branży mediów

społecznościowych byłoby rzeczą nie do pomyślenia, by do pracy na takim poziomie zatrudniać osoby z zewnątrz. Tymczasem restrukturyzację agencji wywiadu w taki sposób, że najbardziej wrażliwe systemy znalazły się pod pieczą osób, które w gruncie rzeczy nie były zatrudnione w agencjach, rząd przedstawiał jako formę innowacji.

Agencje wywiadowcze zatrudniały firmy technologiczne, żeby te zatrudniały dla nich dzieci, którym przekazywano klucze do królestwa, ponieważ – jak tłumaczyły Kongresowi i prasie – nie miały wyboru. Nikt inny nie wiedział, jak owe klucze i w gruncie rzeczy całe królestwo działają. Próbowałem racjonalizować to, czego się dowiedziałem, wmawiając sobie, że to powód do optymizmu. Przełknąłem niedowierzanie, przygotowałem CV i zacząłem odwiedzać targi pracy, bo to one w pierwszych latach XXI wieku były głównym źródłem nowych ofert dla pracowników kontraktowych i miejscem, gdzie firmy najczęściej podkradały rządowy personel. Odbywały się one pod dyskusyjną nazwą *Clearance Jobs*. Sądzę, że tylko mnie bawił fakt, iż słowo wyrażające poświadczenie bezpieczeństwa – *clearance* – mogło również oznaczać wycinkę albo wyburzenie.

W okresie, o którym mowa, targi odbywały się raz w miesiącu w hotelu Ritz-Carlton w Tysons Corner w Wirginii, w niewielkiej odległości od siedziby głównej CIA, albo w jednym z obskurniejszych hoteli w typie Marriotta niedaleko siedziby głównej NSA w Forcie Meade. Z tego, co mi wiadomo, przypominały każdą zwykłą imprezę branżową, z jednym kluczowym wyjątkiem: ciągle odnosiłem wrażenie, że jest tam więcej rekruterów niż potencjalnych rekrutów. Powinno ci to unaocznić, jak wielki apetyt na pracowników panował w branży. Rekruterzy słono płacili za możliwość wystawiania się, ponieważ były to jedyne miejsca w całym

kraju, gdzie każda osoba, która przestępowała próg z przypiętą plakietką z nazwiskiem, w założeniu była wstępnie sprawdzona przez internet, a jej referencje potwierdzone przez agencje – można zatem było założyć, że ma poświadczenie bezpieczeństwa i wymagane umiejętności.

Z chwilą przejścia z ładnie wyposażonego holu do poświęconej wyłącznie biznesowi sali balowej lądowało się na planecie Pracownik Kontraktowy. Wystawiali się tam wszyscy: to już nie był świat Uniwersytetu Stanowego Maryland, tylko takich firm, jak Lockheed Martin, BAE Systems, Booz Allen Hamilton, DynCorp, Titan, CACI, SAIC, COMSO i setek innych o akronimicznych nazwach, z których istnienia nie zdawałem sobie sprawy. Niektórzy wystawcy prezentowali ofertę na stołach, ale największe firmy wabiły pięknie wyposażonymi stoiskami, gdzie można było skosztować przekąsek i napojów.

Po wręczeniu potencjalnemu pracodawcy egzemplarza swojego CV i krótkiej grzecznościowej wymianie zdań, czyli nieformalnej rozmowie kwalifikacyjnej, rekruter wyciągał segregator zawierający listy wszystkich stanowisk rządowych do obsadzenia przez daną firmę. Z racji tego jednak, że oferowana praca miała element tajności, dostępne posady nie były opisane tradycyjnym językiem, lecz niewiele mówiącymi słowami-kluczami. Na dodatek nomenklatura większości firm nie pokrywała się. Na przykład „starszy programista 3” w jednej mógł, ale nie musiał być odpowiednikiem „głównego analityka 2” w innej. Często jedynym sposobem rozróżnienia tych stanowisk było zwrócenie uwagi na wymagania co do doświadczenia, poziomu uprawnień zawodowych i rodzaju poświadczenia bezpieczeństwa.

Po tym, jak w 2013 roku ujawniłem dokumenty wywiadu, rząd amerykański próbował dyskredytować moją osobę, opisując mnie takimi słowami, jak „zwykły pracownik kontraktowy” albo „były pracownik

Della”. Zawierała się w nich sugestia, że miałem mniejsze uprawnienia i dostęp do informacji niż pełnoprawni funkcjonariusze agencji. Kiedy ten kompromitujący opis zdobył wystarczający rozgłos, administracja oskarżyła mnie o „skakanie z kwiatka na kwiatek”, jakbym był niezadowolonym pracownikiem zmieniającym co rusz miejsce pracy, ponieważ nie potrafiłem znaleźć wspólnego języka z przełożonymi albo przerośnięta ambicja kazała mi przeć do przodu, nie zważając na koszty. W rzeczywistości jednak były to wygodne kłamstwa. Środowisko wywiadowcze wie doskonale, że regularne zmiany zatrudnienia to rzecz zupełnie normalna: agencje same doprowadziły do powstania sytuacji, w której od pracowników kontraktowych wymaga się dużej mobilności, bo jest im to na rękę.

Wykonując pracę kontraktową związaną z bezpieczeństwem narodowym, szczególnie w dziedzinie informatyki, często fizycznie spędza się czas w budynku należącym do agencji, jednak oficjalnie – na papierze – jest się członkiem kadry Della, Lockheeda Martina czy innej spośród dziesiątek mniejszych firm, które Dell, Lockeed Martin i podobni regularnie wykupują. Przy okazji takiego przejęcia firma przejmuje, rzecz jasna, również kontrakty, co powoduje, że na twojej wizytówce nagle pojawiają się nowe nazwy pracodawcy i stanowiska. Twoje codzienne obowiązki pozostają jednak te same: wciąż spędzasz czas w agencyjnym biurze i wykonujesz swoje zadania. Nic się nie zmienia. Dziesiątki kolegów siedzących po twojej lewej i prawej stronie – tych samych, którzy codziennie współpracują z tobą przy projektach – mogą, technicznie rzecz biorąc, być pracownikami kilkunastu różnych firm. Każde przedsiębiorstwo od konglomeratów trzymających w garści kontrakty z agencją może dzielić kilka poziomów hierarchii biznesowej.

Żałuję, że nie pamiętam dokładnie porządku chronologicznego mojej kariery pracownika kontraktowego, bo nie mam dostępu do swojego CV – plik ten, o nazwie **Edward_Snowden_Resume.doc**, jest zapisany w folderze **Dokumenty** jednego z moich starych komputerów domowych, dawno zajętych przez FBI. Przypominam sobie jednak, że w mojej pierwszej poważnej pracy kontraktowej byłem w rzeczywistości podwykonawcą: CIA wynajęło firmę BAE Systems Inc., która z kolei skorzystała z usług COMSO, a COMSO zatrudniło mnie.

BAE Systems Inc. to amerykańska spółka-córka brytyjskiego koncernu BAE Systems (powstałego z fuzji British Aerospace oraz zajmującej się produkcją elektroniki i okrętów wojskowych firmy Marconi Electronic Systems), założona specjalnie w celu zdobywania kontraktów od amerykańskich sił wywiadowczych. COMSO zasadniczo pełniło rolę firmy rekrutacyjnej, składało się z kilku osób, które cały czas krążyły po Beltway w poszukiwaniu pracowników kontraktowych („ludzi”) chętnych przyjąć pracę („żeby mieć kim obsadzić biurka”). Spośród firm, z których przedstawicielami miałem okazję rozmawiać na targach pracy, COMSO dawało mi najwięcej, może dlatego, że było jednym z mniejszych przedsiębiorstw. Nigdy nie dowiedziałem się, co oznaczał akronim w nazwie ani czy w ogóle miał jakieś znaczenie. Choć teoretycznie COMSO miało być moim pracodawcą, jak zdecydowana większość pracowników kontraktowych nie przepracowałem nawet dnia w jego biurze ani w żadnym budynku należącym do BAE Systems Inc. Od początku do końca moje biurko znajdowało się w siedzibie głównej CIA.

W rzeczywistości siedzibę COMSO znajdującą się w Greenbelt w stanie Maryland odwiedziłem co najwyżej dwa albo trzy razy w życiu. Podczas jednej z tych wizyt miałem negocjować wynagrodzenie i podpisać różne dokumenty. W CASL-u zarabiałem mniej więcej trzydzieści tysięcy

dolarów rocznie, ale tamta praca nie miała nic wspólnego z informatyką, więc pozbyłem się skrupułów, by zażądać od COMSO pięćdziesięciu tysięcy. Kiedy przedstawiłem tę propozycję facetowi za biurkiem, odpowiedział:

– A co by pan powiedział na sześćdziesiąt?

Byłem wtedy niedoświadczony i nie rozumiałem, dlaczego jest skłonny przepłacać. Sądzę, że zdawałem sobie sprawę, iż pieniądze, które mi oferuje, nie należą w praktyce do COMSO, ale dopiero później pojąłem, że niektóre z kontraktów obsługiwanych przez COMSO, BAE i inne firmy należały do kategorii zwanej „koszty plus". Oznaczało to, że pośrednicy co roku wystawiali agencjom fakturę na wysokość pensji pracownika plus trzy do pięciu procent honorarium. Podnoszenie wynagrodzenia było więc w najlepszym interesie wszystkich zainteresowanych, poza – oczywiście – podatnikami.

Facet z COMSO ostatecznie namówił mnie – a może raczej siebie – na sześćdziesiąt dwa tysiące, w zamian za to, że ponownie zgodziłem się pracować na nocnej zmianie. Podał mi dłoń, a kiedy ją uścisnąłem, przedstawił się jako mój manager. Wyjaśnił następnie, że jego tytuł to tylko formalność, a polecenia będę otrzymywał bezpośrednio z CIA.

– Jeśli wszystko dobrze pójdzie – oznajmił – nigdy więcej się nie spotkamy.

Kiedy słyszy się coś takiego w filmie albo serialu szpiegowskim, zwykle należy rozumieć, że lada moment bohater wyruszy na niebezpieczną misję, podczas której może zginąć. W prawdziwym świecie szpiegostwa znaczy to tyle, co „gratuluję nowej posady". Jestem pewien, że rekruter COMSO zapomniał moją twarz, zanim zamknąłem za sobą drzwi.

Wyszedłem z tego spotkania w radosnym nastroju, ale w drodze powrotnej dopadła mnie szara rzeczywistość: zdałem sobie sprawę, że tak

miał wyglądać mój codzienny dojazd. Jeśli chciałem mieszkać w Ellicott City w stanie Maryland, niedaleko Lindsay, ale pracować dla CIA w Wirginii, musiałbym dwa razy dziennie spędzać do półtorej godziny na zakorkowanej obwodnicy Waszyngtonu, co by mnie wykończyło. Byłem pewien, że krótko po rozpoczęciu pracy zacząłbym odchodzić od zmysłów. W całym wszechświecie nie istniało dość audiobooków, żeby zapełnić ten czas.

Nie mogłem prosić Lindsay, żeby przeniosła się ze mną do Wirginii, bo była dopiero na drugim roku studiów fotograficznych i trzy dni w tygodniu miała zajęcia. Omówiliśmy sytuację, dla bezpieczeństwa nazywając miejsce mojej nowej pracy „COMSO", na przykład: „Dlaczego COMSO musi być tak daleko?". Ostatecznie zadecydowaliśmy, że znajdę małe mieszkanie na miejscu, „niedaleko COMSO" – coś skromnego, gdzie będę mógł przespać się za dnia po nocy przepracowanej „w COMSO" – a w każdy weekend będę wracał do Maryland albo Lindsay będzie przyjeżdżała do mnie.

Wyruszyłem na poszukiwanie odpowiedniego miejsca, czegoś pośrodku części wspólnej diagramu Venna przedstawiającego dwa zbiory mieszkań: tych wystarczająco tanich, by było mnie na nie stać, i tych na tyle ładnych, by Lindsay mogła je znieść. Zadanie okazało się trudne. Kiedy weźmie się pod uwagę, ile osób pracuje dla CIA, i fakt, że siedziba agencji znajduje się w Wirginii, gdzie gęstość zabudowy jest, powiedzmy, zbliżona do tej na terenach wiejskich – nie powinno dziwić, że mieszkania są tam kosmicznie drogie. Kody pocztowe z serii 22100 należą do najkosztowniejszych w całych Stanach.

W końcu znalazłem w serwisie craigslist pokój w cenie zaskakująco dopasowanej do mojego budżetu, w domu znajdującym się zaskakująco blisko – mniej niż piętnaście minut jazdy – siedziby CIA. Pojechałem go obejrzeć, przeświadczony, że zastanę lepiący się od brudu kawalerski

chlew, tymczasem zajechałem przed dużą, ekstrawagancką willę z przeszklonym frontem i nieskazitelnie zadbanym trawnikiem ozdobionym starannie przyciętymi krzewami i świątecznymi lampkami. Daję słowo, że kiedy szedłem w stronę drzwi wejściowych, miałem coraz silniejsze wrażenie, że czuję zapach przypraw korzennych.

Otworzył mi facet o imieniu Gary. Po e-mailu rozpoczynającym się od słów „Drogi Edwardzie", który od niego dostałem, domyśliłem się, że będzie starszy, ale nie spodziewałem się, że spotkam kogoś tak szykownie ubranego. Gary był bardzo wysoki, miał krótko ścięte siwe włosy; na garnitur włożył fartuch kuchenny. Spytał mnie bardzo uprzejmie, czy mógłbym chwilę poczekać, bo jest akurat zajęty w kuchni. Przygotowywał całą blachę pieczonych jabłek; najpierw powtykał w nie goździki, a potem posypał je z wierzchu ogromną ilością gałki muszkatołowej, cynamonu i cukru.

Kiedy jabłka trafiły do piekarnika, Gary zaprowadził mnie do pokoju mieszczącego się w suterenie, i wyjaśnił, że mogę wprowadzić się od zaraz. Przystałem na tę propozycję i wpłaciłem kaucję oraz czynsz za pierwszy miesiąc. Następnie Gary przedstawił mi zasady obowiązujące w domu:

Żadnego bałaganu.

Żadnych zwierząt.

Żadnych gości na noc.

Muszę przyznać, że pierwszą regułę złamałem prawie natychmiast. Naruszaniem drugiej nigdy nie byłem zainteresowany w najmniejszym nawet stopniu. Jeśli zaś chodzi o trzecią, to dla Lindsay Gary zrobił wyjątek.

13_Indoc|

Być może zwróciłeś uwagę na charakterystyczne ujęcie wprowadzające, wykorzystywane w większości szpiegowskich filmów i seriali: na ekranie pojawia się napis „Kwatera główna CIA, Langley, Wirginia”, po czym kamera sunie przez wyłożony marmurami hol, ukazując ścianę z gwiazdami oraz godło agencji na posadzce. W rzeczywistości Langley to historyczna nazwa, którą upodobali sobie filmowcy z Hollywood; formalnie rzecz biorąc, kwatera główna CIA znajduje się w McLean w stanie Wirginia. A przez marmurowy hol przechodzą dziś niemal wyłącznie VIP-y oraz wycieczki.

Budynek, dokąd CIA zaprasza filmowców i oficjeli, to Stara Kwatera Główna, nazywana potocznie OHB (skrót od Old Headquarters Building). Większość pracowników CIA urzęduje natomiast w sąsiednim, niedostępnym dla kamer i osób postronnych budynku, zwanym NHB (New Headquarters Building, Nowa Kwatera Główna). Mój pierwszy dzień był zarazem jednym z niewielu, jakie przepracowałem tam na dziennej zmianie. Nawiasem mówiąc, nie oznaczało to wcale pracy przy dziennym świetle, bo większość czasu spędziłem pod ziemią, w nieco zapuszczonej sali o nieotynkowanych ścianach z pustaków. Pomieszczenie to było równie przytulne, co schron przeciwatomowy, a w powietrzu unosił się zapach środka dezynfekującego.

– A więc to tak wygląda państwo w państwie – stwierdził jeden z obecnych w sali mężczyzn, na co prawie wszyscy pozostali wybuchnęli śmiechem.

Facet spodziewał się zapewne, że w podziemiach kwatery głównej CIA natknie się na gromadę WASP-ów*, absolwentów Ligi Bluszczowej, którzy zarzucą na głowy kaptury, uformują krąg i zaczną śpiewać monotonnym głosem dziwne pieśni. Ja z kolei przypuszczałem, że spotkam tam typowych przedstawicieli klasy urzędniczej, czyli jakby młodszą wersję moich rodziców. Okazało się jednak, że zgromadzone w podziemnej sali towarzystwo składało się z samych komputerowców. Siedzący wokół mnie prawie sami młodzi mężczyźni – kobiet było wśród nas jak na lekarstwo – najwyraźniej po raz pierwszy w życiu założyli ubrania w stylu *business casual*. Wielu miało na ciele tatuaże i kolczyki albo ślady po kolczykach wyjętych zapewne na okazję pierwszego dnia w pracy; jeden z chłopaków miał nawet punkowe, kolorowe pasemka we włosach. Niemal wszyscy nosiliśmy wydawane kontraktowym pracownikom CIA identyfikatory, zielone i sztywne jak nowe studolarówki. Z całą pewnością nie wyglądaliśmy na opętanych rządzą władzy członków tajnej koterii, którzy z ukrytych głęboko pod ziemią biurowych boksów kontrolują poczynania demokratycznie wybranych przedstawicieli narodu.

Spotkanie w przypominającym schron pomieszczeniu miało być pierwszym etapem naszej transformacji. Nosiło nazwę Indoc – od *indoctrination* (indoktrynacji); było to szkolenie formacyjne, służyło przede wszystkim wpojeniu nam przekonania, że należymy do elitarnego grona wybrańców, godnego uzyskania wglądu w tajemnice państwowe oraz poznania prawd, jakich nie można wyjawić zwykłym obywatelom, a w niektórych wypadkach nawet przedstawicielom władzy ustawodawczej i sądowniczej.

Kiedy słuchałem wywodów prowadzących szkolenie instruktorów, nie mogłem oprzeć się wrażeniu, że wyważają oni otwarte drzwi, starając się przekonać nas o czymś, o czym i tak byliśmy już święcie przekonani. Nie

ma potrzeby utwierdzać speca od komputerów w przeświadczeniu, że posiada wyjątkową wiedzę i umiejętności, które dają mu prawo do działania według własnego uznania i podejmowania decyzji w imieniu współobywateli, bez żadnego nadzoru z ich strony. Nic nie rozbudza w nas arogancji równie skutecznie jak sprawowanie kontroli nad maszynami niezdolnymi do krytycznej oceny naszych działań.

Na tym właśnie, jak sądzę, polega zasadnicze podobieństwo między światem rządowych agencji wywiadowczych i światem nowych technologii. Podmioty z obu tych rzeczywistości posiadają realną władzę bez demokratycznego mandatu, a także szczycą się tym, że utrzymują swoje działania w ścisłej tajemnicy. Żywią też przeświadczenie, że są w stanie znaleźć rozwiązanie każdego problemu i nie wahają się podejmować jednostronnych decyzji o wprowadzeniu tych rozwiązań w życie. A przede wszystkim wierzą, że rozwiązania te są z natury apolityczne, ponieważ opierają je na twardych danych, stanowiących prerogatywę nad chaotycznymi wyborami i decyzjami przeciętnego obywatela.

Wejście do świata Wspólnoty Wywiadów (Intelligence Community, IC), podobnie zresztą jak nabycie eksperckiej wiedzy w dziedzinie nowoczesnych technologii, wywiera silny wpływ na ludzką psychikę. Nagle zyskujesz dostęp do informacji, dzięki którym niespodziewanie dostrzegasz zupełnie nowy wymiar wielu faktów; możesz zajrzeć za kulisy znanych lub pozornie znanych historycznych wydarzeń. Niektórzy, zwłaszcza abstynenci tacy jak ja, mogą wręcz poczuć się tym wszystkim upojeni. Poza tym z chwilą rozpoczęcia pracy dla wywiadu zyskujesz nie tyle przyzwolenie, co wręcz obowiązek kłamania, zwodzenia, przemilczania i zatajania. W rezultacie u pracowników wywiadu rodzi się silne poczucie plemiennej przynależności; często prowadzi ono do

przekonania, że lojalność wobec instytucji, dla której pracują, jest ważniejsza od wierności prawu.

Oczywiście żadna z tych refleksji nie naszła mnie w trakcie szkolenia formacyjnego. Tamtego dnia starałem się po prostu nie zasnąć z nudów. Prowadzący Indoc zapoznawali nas z podstawowymi zasadami bezpieczeństwa, będącymi częścią stosowanych w pracy wywiadowczej technik operacyjnych; określano je zbiorczo mianem *tradecraft*, czyli szpiegowskie rzemiosło. Wiele z tych zasad było tak oczywistych, że kiedy tego słuchałem, mój umysł ogarniało otępiające znużenie. Nie mów nikomu, dla kogo pracujesz. Nie zostawiaj poufnych dokumentów bez nadzoru. Nie przynoś prywatnego niezabezpieczonego telefonu komórkowego do biura, gdzie obowiązują najwyższe standardy bezpieczeństwa – i nigdy, pod żadnym pozorem, nie korzystaj z prywatnego telefonu do prowadzenia rozmów dotyczących pracy. Nie paraduj po centrum handlowym z dyndającym na piersi służbowym identyfikatorem, bo to zupełnie tak, jakbyś mówił wszystkim dookoła „Cześć, pracuję dla CIA”.

W końcu długa litania przykazań dobiegła końca. Prowadzący szkolenie zgasili światło i uruchomili PowerPointa, po czym na przymocowanym do ściany ekranie zaczęły pojawiać się twarze. Wszyscy momentalnie zostaliśmy wyrwani z letargu. Poinformowano nas, że patrzymy właśnie na zdjęcia byłych agentów i pracowników kontraktowych, którzy – z powodu chciwości, niekompetencji lub niedbalstwa, a czasem ze zwykłej złośliwości – złamali obowiązujące w agencjach wywiadowczych zasady. Pycha pozwoliła im uwierzyć, że stoją ponad tymi zasadami, po czym zaprowadziła ich za kraty i zrujnowała im życie. Dano nam do zrozumienia, że wszyscy ci ludzie przebywają obecnie w lochach znacznie gorszych od

tego, gdzie odbywało się nasze szkolenie, a niektórzy z nich pozostaną tam do końca swoich dni.

Ogólnie rzecz biorąc, była to całkiem skuteczna prezentacja.

Słyszałem, że w kolejnych latach, już po zakończeniu mojej kariery w służbach wywiadowczych, do tej galerii zdjęć niekompetentnych nieudaczników, zdrajców oraz kretów obcych służb dodana została jeszcze jedna kategoria przeniewierców. Obejmuje ona demaskatorów, którzy ujawnili nielegalne działania służb, kierując się interesem publicznym. Mogę tylko mieć nadzieję, że kiedy podczas odbywających się dziś szkoleń na ekranie pojawiają się twarze różnej maści renegatów – a wśród nich także i moja – dwudziestoparoletni adepci wywiadu dostrzegają rażącą niesprawiedliwość – zrównywanie tych, którzy sprzedali państwowe tajemnice wrogom, z tymi, którzy ujawnili je dziennikarzom.

Pracę w CIA rozpocząłem wtedy, gdy morale w agencji sięgnęło dna. W następstwie błędów popełnionych przez amerykańskie służby wywiadowcze przed 11 września 2001 roku Kongres oraz rząd Stanów Zjednoczonych rozpoczęli szeroko zakrojoną akcję reorganizacyjną. Polegała ona między innymi na pozbawieniu dyrektora Centrali Wywiadu podwójnej roli szefa CIA oraz zwierzchnika wszystkich rządowych służb wywiadowczych wchodzących w skład Wspólnoty Wywiadów; funkcję dyrektora Centrali Wywiadu pełnił każdy kolejny dyrektor CIA od czasu utworzenia agencji w roku 1947. Wraz z wymuszoną przez władze rezygnacją George’a Teneta ze stanowiska dyrektora Centrali Wywiadu zakończył się trwający ponad pół wieku okres supremacji CIA nad pozostałymi agencjami wywiadowczymi.

W szeregach CIA odejście Teneta i ograniczenie kompetencji dyrektora agencji uznano za symbol zdrady, jakiej dopuściła się klasa polityczna w stosunku do CIA. Wśród pracowników agencji powszechne było

poczucie, że padli ofiarą manipulacji ze strony administracji Busha, która wykorzystała CIA do realizacji swoich celów, a następnie obarczyła ją winą za swoje największe nadużycia. W CIA zaczęły nasilać się martyrologiczne nastroje i atmosfera oblężonej twierdzy. Negatywne emocje podsyciła jeszcze nominacja na dyrektora agencji Portera Gossa – niczym niewyróżniającego się byłego oficera CIA, który po zakończeniu służby w wywiadzie wstąpił do Partii Republikańskiej i jakiś czas później został kongresmenem z Florydy. Goss był pierwszym dyrektorem CIA piastującym to stanowisko w nowym, zredukowanym wymiarze. Obsadzenie na stanowisku szefa CIA czynnego polityka zostało odebrane przez pracowników agencji jako swoista kara i próba poddania wywiadu partyjnej kontroli oraz zapowiedź dalszych kroków, mających na celu uczynienie z niego narzędzia w rękach republikańskiej administracji. Dyrektor Goss niezwłocznie przystąpił do redukcji zatrudnienia, zwalniając wielu etatowych pracowników lub zmuszając ich do przejścia na wcześniejszą emeryturę. W rezultacie CIA zaczęła cierpieć na poważne braki kadrowe i stała się jeszcze bardziej zależna od pracowników kontraktowych. Ocena działań CIA przez społeczeństwo amerykańskie jeszcze nigdy w historii nie była tak niska jak wówczas; nigdy też opinia publiczna nie miała tak dokładnego wglądu w wewnętrzne mechanizmy funkcjonowania agencji – był to skutek licznych przecieków na temat utrzymywania przez CIA tajnych więzień i prowadzenia operacji w trybie nadzwyczajnym.

W tamtym czasie struktura organizacyjna agencji obejmowała pięć wydziałów. Dyrekcja Operacji odpowiadała za działalność *stricte* szpiegowską. W Dyrekcji Wywiadu syntetyzowano i analizowano informacje zdobyte przez szpiegów. Dyrekcja Nauki i Techniki zajmowała się projektowaniem i konstruowaniem komputerów, środków łączności oraz

broni; zaopatrywała pozostałe wydziały, a także prowadziła szkolenia z obsługi tego sprzętu. Dyrekcja Administracji składała się z prawników, pracowników działu kadr, a także logistyków odpowiedzialnych za koordynowanie codziennej działalności; zadaniem tego wydziału było także utrzymywanie stałych kontaktów z administracją rządową. Dyrekcja Wsparcia była najdziwniejszym, a zarazem największym wówczas wydziałem. Kierowała całym personelem pomocniczym, począwszy od większości inżynierów i lekarzy aż po pracowników kawiarni, siłowni oraz służb ochrony w obiektach należących do CIA. Najważniejszym zadaniem Dyrekcji Wsparcia było jednak zarządzanie globalną infrastrukturą telekomunikacyjną agencji – platformą, za której pośrednictwem informacje zebrane przez agentów wywiadu spływały do pionu analitycznego, a raporty analityków docierały do pionu administracyjnego. Pracownicy tego wydziału zapewniali niezbędne wsparcie techniczne wszystkim pozostałym jednostkom organizacyjnym CIA, sprawowali opiekę nad serwerami i czuwali nad ich bezpieczeństwem – ich zadanie polegało na tworzeniu, obsłudze i ochronie całej sieci teleinformatycznej CIA, a także zapewnianiu łączności z sieciami innych agencji rządowych oraz kontrolowaniu dostępu do zasobów sieci CIA. Krótko mówiąc, byli to specjaliści, którzy za pomocą nowoczesnej techniki spajali wszystko w jedną całość. Nie powinien zatem dziwić fakt, że większość z nich stanowili ludzie młodzi, ani to, że w zdecydowanej większości byli to pracownicy kontraktowi.

To właśnie Dyrekcji Wsparcia podlegał zespół, w którym przyszło mi pracować. Naszym zadaniem było zarządzanie architekturą serwerową CIA na obszarze metropolitalnym Waszyngtonu, czyli większością serwerów utrzymywanych przez agencję w kontynentalnej części Stanów Zjednoczonych. Nadzorowaliśmy ogromne serwerownie pełne wartych

krocie komputerów typu mainframe, których twarde dyski przechowywały zasoby wewnętrznych sieci oraz bazy danych CIA. Odpowiadaliśmy za prawidłowe funkcjonowanie i bezpieczeństwo wszystkich systemów służących przekazywaniu, odbieraniu i przechowywaniu informacji wywiadowczych. Wprawdzie agencja posiadała liczne, rozsiane po całym kraju serwery przekaźnikowe, jednak wiele spośród najważniejszych z nich znajdowało się w jej kwaterze głównej w Wirginii. Połowa ulokowana była w budynku NHB, gdzie urzędował także nasz zespół, a druga połowa w sąsiednim budynku OHB. Serwerownie mieściły się po przeciwległych stronach obu siedzib, tak aby w razie wysadzenia w powietrze jednej z serwerowni nie doszło do utraty zbyt wielu cennych maszyn.

Mój certyfikat dostępu do informacji niejawnych określonych klauzulą „ściśle tajne” (TS/SCI) obejmował kilka różnych „kategorii” informacji, między innymi SIGINT (informacje pozyskane dzięki przechwyceniu komunikacji odbywającej się różnymi kanałami łączności elektronicznej lub radiowej), a także HUMINT (informacje zdobyte przez wywiad agenturalny, a także wszelkie dane zawarte w raportach sporządzanych przez agentów oraz analityków). Pozyskiwanie danych z kanałów łączności oraz klasycznymi metodami szpiegowskimi to standardowe działania CIA. Oprócz tego zostałem dopuszczony do informacji z kategorii COMSEC (czyli dotyczących bezpieczeństwa łączności), dzięki czemu mogłem mieć kontakt z tajnymi materiałami kryptograficznymi. Szyfry uważane są powszechnie za największą i najpilniej strzeżoną tajemnicę każdej agencji wywiadowczej, ponieważ służą do ochrony wszelkich innych tajemnic. Materiały kryptograficzne, wykorzystywane przez CIA do szyfrowania informacji i danych, przechowywano na zarządzanych przeze mnie serwerach. Mój zespół był jednym z niewielu w całej agencji posiadającym

fizyczny dostęp do tych maszyn i prawdopodobnie jedynym, który mógł logować się do większości z nich.

W CIA bezpieczne biura nazywane są „kryptami”; do krypty mojego zespołu prowadził hol, gdzie rezydowała sekcja pomocy technicznej. Jej personel sekcji mający zawsze pełne ręce roboty składał się z osób w wieku zbliżonym do moich rodziców. Większość zatrudnionych tam mężczyzn nosiła marynarki i bawełniane spodnie, natomiast kobiety ubierały się przeważnie w bluzki i spódnice; w owym czasie było to jedno z nielicznych miejsc w zdominowanej przez nowoczesne technologie kwaterze głównej CIA, w którym widywałem regularnie większą liczbę kobiet. Spora część pracowników pomocy technicznej posiadała niebieskie identyfikatory przysługujące pracownikom agencji na etacie rządowym, czyli – jak nazywali ich kontraktowi – „budżetowcom”. Ich praca polegała na odbieraniu dzwoniących nieustannie telefonów i zapewnianiu pomocy rozmówcom telefonującym z biur kwatery głównej albo z placówek CIA w terenie w rozwiązywaniu rozmaitych problemów natury technicznej. Było to coś w rodzaju wywiadowczej wersji biura obsługi klienta. Telefoniczni konsultanci resetowali hasła, odblokowywali zablokowane konta i recytowali wyuczone na pamięć formułki: „Czy możesz się wylogować i zalogować ponownie?”; „Czy kabel sieciowy jest podłączony?”. Jeśli oni, posiadający zazwyczaj minimalną wiedzę na tematy techniczne, nie byli w stanie poradzić sobie z jakimś problemem, łączyli rozmówcę z bardziej wyspecjalizowanym zespołem; robili to zwłaszcza wtedy, gdy kłopot wystąpił w jednej z zagranicznych placówek CIA – w Kabulu, Bagdadzie, Bogocie czy w Paryżu.

Muszę ze wstydem przyznać, że kiedy po raz pierwszy mijałem biurka sekcji pomocy technicznej, rozpierała mnie duma. Byłem o kilka dekad młodszy od siedzących przy nich budżetowców, a mimo to zmierzałem

pewnym krokiem do krypty, do której oni nie mieli i nigdy nie będą mieć wstępu. Wtedy nie przyszło mi jeszcze do głowy, że taka sytuacja może świadczyć o dysfunkcji całego systemu – o tym, że nasz rząd zupełnie odpuścił sobie wyszukiwanie utalentowanych kandydatów na nowe stanowiska wśród własnych pracowników, ponieważ łatwiej i prościej było zatrudniać specjalistów na kontraktach. Codzienne mijanie przeze mnie starszych pracowników pomocy technicznej w drodze do krypty stało się dla mnie najbardziej wymownym symbolem dokonującej się we Wspólnocie Wywiadów pokoleniowej i kulturowej zmiany – zmiany, której sam byłem częścią. O polityce zatrudnienia w amerykańskich agencjach wywiadowczych decydowali od zawsze członkowie waszyngtońskich koterii, wywodzący się ze środowiska finansowej i przemysłowej elity. Zdawali sobie oni sprawę z konieczności nadążania za rozwojem nowoczesnych technologii, a zarazem nie mieli najmniejszej ochoty, by próbować je zrozumieć; postanowili więc ułatwić sobie życie i zaprosili do rządowych agencji młodych hakerów i powierzyli im nieskrępowany dostęp do niezwykle zaawansowanych systemów bezpieczeństwa i kontroli oraz pełną pieczę nad nimi.

Z czasem szczerze polubiłem budżetowców z sekcji pomocy technicznej. Zawsze odnosili się do mnie z życzliwością i sympatią i doceniali moją gotowość do służenia im pomocą w każdej sytuacji, także wtedy, gdy nie należało to do moich obowiązków. Sam również wiele im zawdzięczałem: dzięki codziennym rozmowom, w których dzielili się ze mną wiedzą i doświadczeniami, stopniowo zacząłem lepiej rozumieć mechanizmy funkcjonowania agencji jako organizacji wykraczającej swoją działalnością daleko poza dobrze mi znane okolice Beltway. Wielu pracowników sekcji pomocy technicznej miało za sobą służbę w zagranicznych placówkach CIA w charakterze agentów wywiadu – takich

samych jak ci, którym obecnie pomagali przez telefon rozwiązywać drobne techniczne problemy. Lata spędzane za granicą nierzadko odbijały się negatywnie na ich życiu rodzinnym, a kiedy w końcu wracali do kraju, czekało ich zesłanie do pomocy technicznej. Mieli tam tkwić za biurkiem aż do emerytury, ponieważ nie posiadali umiejętności komputerowych i informatycznych, czyli tych najbardziej cenionych w agencji coraz bardziej skupionej na rozwijaniu potencjału technologicznego.

Cieszył mnie szacunek, jaki zaskarbiłem sobie u budżetowców z tego działu. Nie podobało mi się protekcjonalne współczucie, z jakim wypowiadano się o nich w moim zespole; jeszcze bardziej drażnił mnie fakt, że niektórzy koledzy nabijali się z tych inteligentnych i oddanych swojej pracy ludzi – kobiet i mężczyzn, którzy w zamian za niską pensję i szczyptę chwały poświęcili agencji wiele lat życia, często w niegościnnych, a nawet niebezpiecznych zakątkach świata, i których w ramach podziękowania za wierną służbę oddelegowano do odbierania telefonów w zapyziałym korytarzu.

Po kilku tygodniach przepracowanych na dziennej zmianie i po zapoznaniu się z działaniem systemów, za które byłem odpowiedzialny, zostałem przeniesiony na nocną zmianę trwającą od szóstej wieczorem do szóstej rano. O tej porze budynek Nowej Kwatery Głównej był niemal zupełnie opustoszały, wyjątkiem były stanowiska sekcji pomocy technicznej, gdzie dyżurowała garstka ziewających dyskretnie konsultantów.

Nocami, zwłaszcza między godziną dwudziestą drugą a czwartą nad ranem, rozległy kompleks kwatery głównej CIA sprawiał postapokaliptyczne wrażenie. Wszystkie ruchome schody były wyłączone. Działała jedynie połowa wind, a dzwonek towarzyszący otwieraniu i zamykaniu drzwi, który za dnia było ledwo słyszalny, w nocy wydawał się

niepokojąco głośny. Poprzedni dyrektorzy rzucali surowe spojrzenia z wiszących na ścianach portretów, a rzeźby bielików amerykańskich przypominały żywe drapieżniki, zastygłe w bezruchu i gotowe w każdej chwili rzucić się na ofiarę. Amerykańskie flagi wyglądały jak zjawy w czerwono-biało-niebieskich prześcieradłach. Nieco wcześniej agencja wdrożyła nowy program oszczędzania energii i zainstalowała oświetlenie włączane przez czujniki ruchu. Kiedy szedłem korytarzem, miałem przed sobą pogrążoną w ciemnościach czeluść, a kolejne lampy zapalały się dopiero wtedy, gdy zbliżałem się do nich na odpowiednią odległość; w rezultacie przez cały czas czułem się śledzony, a nieprzyjemne uczucie potęgował odbijający się echem odgłos moich kroków.

Zmiana trwała dwanaście godzin; po trzech dniach pracy przysługiwały mi dwa dni wolnego. Większość czasu spędzałem w bezpiecznym biurze mieszczącym się za stanowiskiem pomocy technicznej. Na każdym z dwudziestu biurek stały po dwa lub trzy terminale komputerowe obsługiwane przez administratorów systemu, których zadaniem było utrzymanie ciągłości działania globalnej sieci CIA. Może brzmi to skomplikowanie, ale w rzeczywistości moja praca była dość banalna – sprowadzała się w gruncie rzeczy do oczekiwania na awarię. Pojawiające się od czasu do czasu problemy nie były zazwyczaj trudne do usunięcia. Kiedy coś się zepsuło, logowałem się do odpowiedniego serwera, żeby spróbować naprawić usterkę zdalnie. Jeśli nie byłem w stanie tego zrobić, musiałem własnoręcznie pomajstrować przy szwankującej maszynie. W tym celu byłem zmuszony zejść do mieszczącego się piętro niżej centrum danych; jeśli mankament występował w centrum danych w Starej Kwaterze Głównej, czekał mnie półkilometrowy, nieco upiorny spacer podziemnym tunelem łączącym budynki NHB i OHB.

Moim partnerem na nocnej zmianie – i zarazem jedyną oprócz mnie osobą czuwającą nocami nad prawidłowym funkcjonowaniem całej architektury serwerowej CIA – pozostawał gość, którego będę tu nazywał Frankiem. Pięćdziesięcioparoletni Frank był najbardziej nietypowym członkiem zespołu odpowiedzialnego za serwery i osobą pod każdym względem niezwykłą. Miał sprecyzowane poglądy polityczne (był libertarianinem i to tak radykalnym, że wszystkie oszczędności lokował w złotych krugerrandach), a jego zainteresowania wykraczały poza technikę (był zapalonym czytelnikiem starych thrillerów i kryminałów). Za młodu służył jako radiooperator w marynarce wojennej; karierę w CIA rozpoczął w sekcji pomocy technicznej, ale ponieważ był pracownikiem kontraktowym, zaproponowano mu przejście na lepsze stanowisko.

Przyznaję, że kiedy go poznałem, pomyślałem: „Wyobraź sobie, że całe twoje życie miałoby wyglądać jak te nocki w CASL-u”. Powiedzmy sobie szczerze, Frank nie robił prawie nic. A przynajmniej lubił sprawiać takie wrażenie. Z upodobaniem opowiadał mi o tym, że kompletnie nie zna się na komputerach i nie ma pojęcia, dlaczego przydzielono go do tak ważnego zespołu. Często powtarzał, że „wdrożenie systemu pracowników kontraktowych to trzeci największy przekręt, jaki zrobiono w Waszyngtonie”; dwa pozostałe to, zdaniem Franka, wprowadzenie podatku dochodowego oraz sam fakt istnienia Kongresu Stanów Zjednoczonych. Twierdził też, że kiedy otrzymał propozycję przejścia do zespołu zajmującego się serwerami, przestrzegał swojego przełożonego, że nie będzie tam z niego żadnego pożytku – ale i tak go tam przeniesiono. Frank zapewniał mnie, że przez większą część ostatnich dziesięciu lat zajmował się w pracy wyłącznie czytaniem książek; mogę jednak zaświadczyć, że czasem układał też pasjansa – rzecz jasna nie na komputerze, lecz posługując się prawdziwą talią kart – oraz wspominał byłe

żony („był z niej prawdziwy anioł”) i dziewczyny („ukradła mi samochód, ale i tak warto było”). Zdarzało mu się też spędzić całą noc na chodzeniu tam i z powrotem i odświeżaniu co chwilę konserwatywnego portalu Drudge Report.

Kiedy Frank odbierał telefon z informacją o usterce, a potrząsanie zepsutym serwerem nie przynosiło żadnego efektu, ograniczał się do poinformowania o awarii kolegów z dziennej zmiany. Jego filozofia (o ile można to tak nazwać) sprowadzała się do tego, że nocna zmiana prędzej czy później dobiegnie końca, a dzienna ma na tyle liczne zasoby ludzkie, że z pewnością da sobie radę. Najwyraźniej jednak ludzie pracujący za dnia mieli w końcu dość tego, że codziennie rano po przyjściu do biura musieli rozwiązywać problemy, w których sprawie Frank przez całą noc nawet nie kiwnął palcem – i tak oto trafiłem na nocną zmianę.

Z jakiegoś powodu w agencji uznano, że lepiej będzie przydzielić temu starszemu facetowi mnie do pomocy niż po prostu go zwolnić. Po kilku przepracowanych razem tygodniach nabrałem podejrzeń, że Frank trzyma się swojej posady wyłącznie dzięki osobistym koneksjom. Żeby zweryfikować tę hipotezę, zagadnąłem go kiedyś, z którym dyrektorem lub inną szychą z CIA służył razem w marynarce. Frank wygłosił wtedy długą przemowę o tym, że żaden z wysoko postawionych w hierarchii CIA weteranów marynarki wojennej nie był zwykłym marynarzem – wszyscy służyli w randze oficera, co jego zdaniem wyjaśniało fatalne wyniki agencji.

Nagle przerwał tyradę, a na jego twarzy odmalowała się panika. Zerwał się na równe nogi.

– Muszę zmienić taśmę! – zawołał.

Nie miałem pojęcia, co ma na myśli. Ale Frank zmierzał już w kierunku szarych drzwi na samym końcu krypty. Było to wyjście na obskurną klatkę

schodową prowadzącą do znajdującego się bezpośrednio pod naszym biurem centrum danych – mrocznej sali wypełnionej lodowatym powietrzem i nieustannym monotonnym szumem.

Po wejściu do serwerowni – zwłaszcza do tej CIA – człowiek może poczuć się nieco zdezorientowany. Otacza cię ciemność, w której błyskają zielone i czerwone kontrolki LED niczym lampki choinkowe w jakiejś złowróżbnej parodii świąt Bożego Narodzenia; powietrze wibruje za sprawą przemysłowych wentylatorów chłodzących umieszczone w specjalnych szafach bezcenne serwery i chroniących je przed roztopieniem. Pobyt w tym miejscu zawsze przyprawiał mnie o lekki zawrót głowy – a co dopiero pobyt w towarzystwie klnącego jak marynarz starszego faceta, przemierzającego serwerownię szybkim krokiem.

Frank zatrzymał się w kącie, gdzie stał prowizoryczny biurowy boks sklecony z materiałów należących kiedyś do Dyrekcji Operacji, o czym świadczyły umieszczone na ściankach oznaczenia. Wewnątrz znajdowało się tandetne, rozlatujące się biurko, na nim stał stary komputer. Przyjrzawszy mu się uważniej, doszedłem do wniosku, że musiał to być sprzęt z początku lat dziewięćdziesiątych, a może nawet z końca lat osiemdziesiątych, starszy niż wszystkie komputery, jakie widywałem w pracowni mojego ojca w Straży Wybrzeża – tak stary, że na dobrą sprawę nie zasługiwał na miano komputera. Była to raczej maszyna wyposażona w miniaturową taśmę, której formatu nie potrafiłem rozpoznać, ale byłem niemal pewien, że Instytut Smithsoński chętnie włączyłby ją do swoich muzealnych zbiorów.

Obok tej antycznej machiny stał masywny sejf. Frank otworzył go, po czym przez moment mocował się z taśmą znajdującą się w maszynie. Kiedy już udało mu się ją wyjąć, schował ją do sejfu. Następnie wyciągnął z niego nową taśmę, umieścił ją w urządzeniu i przewlekł w odpowiedni sposób

końcówkę taśmy, nawet na nią nie spoglądając i posługując się samym tylko dotykiem. Potem kilkakrotnie nacisnął klawisze na starej klawiaturze – strzałka w dół, strzałka w dół, strzałka w dół, tabulator, tabulator, tabulator. Monitor maszyny był zepsuty, więc nie można było obserwować efektów naciskania klawiszy, ale niezrażony tym Frank bez wahania nacisnął Enter.

Maleńka taśma drgnęła kilka razy, po czym zaczęła się obracać, a Frank uśmiechnął się zadowolony.

– To najważniejsza maszyna w całym budynku – oświadczył. – Agencja nie ufa tej gównianej technologii cyfrowej. Nie ufają własnym serwerom. Sam zresztą wiesz, że ciągle się psują. Kiedy serwer ma awarię, istnieje ryzyko, że agencja straci to, co na nim przechowuje. Żeby nie stracić niczego, co napłynęło do nas przez cały dzień, w nocy kopiuje się wszystko na taśmę.

– Czyli robisz tu kopie zapasowe danych?

– Kopie zapasowe na taśmie. Stara szkoła. Taśma prawie nigdy nie nawala.

– Ale co dokładnie? Informacje na temat personelu, nadesłane dane wywiadowcze?

Frank przyłożył rękę do brody, tak jakby się nad czymś zastanawiał, i udawał, że potraktował moje pytanie poważnie.

– Ed, chłopie, nie chciałem ci tego mówić – odezwał się po chwili. – To były raporty od twojej dziewczyny. Surowe dane wywiadowcze. Bardzo surowe.

Śmiejąc się, wrócił po schodach do naszej krypty, zostawiając mnie zaczerwienionego i speszonego w półmroku serwerowni.

Kiedy Frank przeprowadził tę procedurę zmiany taśmy nazajutrz, a potem robił to każdej kolejnej nocy, zacząłem wreszcie rozumieć,

dlaczego agencja nie zdecydowała się go pozbyć – i wcale nie chodziło wyłącznie o jego poczucie humoru. Był po prostu jedyną osobą w agencji gotową pracować od szóstej wieczorem do szóstej nad ranem, a zarazem potrafiącą obsługiwać system taśmowego zapisu danych. Wszyscy inni technicy, którzy pamiętali te zamierzchłe czasy, kiedy taśmy były popularnym nośnikiem danych, zdążyli pozakładać rodziny i woleli spędzać wieczory w domu, ze swoimi bliskimi. Frank natomiast pozostał kawalerem, a do tego pamiętał czasy jeszcze sprzed oświecenia.

Odkąd znalazłem sposób na zautomatyzowanie znacznej części mojej pracy – napisałem skrypty umożliwiające automatyczne uaktualnianie oprogramowania serwerów oraz przywracanie utraconego połączenia z siecią – miałem do dyspozycji równie wiele wolnego czasu, co Frank. Innymi słowy, mogłem przez całą noc robić to, na co miałem ochotę. Wiele godzin przegadałem z Frankiem; najczęściej dyskutowaliśmy o jego politycznych lekturach, na przykład o książkach postulujących powrót Ameryki do standardu złota albo omawiających wady i zalety podatku liniowego. Ale każdej nocy były godziny, kiedy Frank znikał – albo zaszywał się gdzieś z nosem w jednej z powieści kryminalnych i czytał aż do rana, albo wyruszał na przechadzkę po opustoszałych korytarzach, zaglądając po drodze do kantyny, żeby zjeść kawałek pizzy, albo do siłowni, żeby trochę poćwiczyć. Ja miałem własny sposób na spędzanie wolnego czasu. Buszowałem w sieci.

Kiedy wchodzisz do internetu z placówki CIA, musisz wyrazić zgodę na monitorowanie twojej aktywności online – zaznaczając odpowiednią opcję, zgadzasz się na to, że wszystko, co robisz, jest rejestrowane, i zrzekasz się prawa do prywatności. Zgodę tę wyrażasz na tyle często, że wchodzi ci to w nawyk i w końcu robisz to machinalnie. Chcesz po prostu jak najszybciej pozbyć się wyskakującego co rusz okienka i wrócić do

swoich zajęć. Moim zdaniem jest to główny powód, dlaczego osoby pracujące w agencjach wywiadowczych nie podzielają obaw cywilów o bycie śledzonym w sieci. Nie chodzi o to, że pracownicy wywiadu mają dostęp do jakichś poufnych danych dowodzących, że cyfrowa inwigilacja w znaczący sposób poprawia bezpieczeństwo Ameryki – po prostu zdążyli przyzwyczaić się do tego, że ich szef ma wgląd do wszystkiego, co robią w internecie.

Poza tym w publicznym internecie wcale nie ma aż tak wielu ciekawych rzeczy, których nie byłoby w zasobach wewnętrznej sieci agencji. Mało kto zdaje sobie sprawę, że CIA posiada własny internet i własną sieć Web. Dysponuje także odpowiednikiem Facebooka, pozwalającym pracownikom CIA nawiązywać i utrzymywać ze sobą kontakty towarzyskie, a także odpowiednikiem Wikipedii, zapewniającym dostęp do informacji na temat zespołów, projektów i misji prowadzonych przez agencję. Wewnętrzny ekwiwalent wyszukiwarki Google – dostarczony przez firmę Google – umożliwia wygodne przeszukiwanie zasobów tajnej sieci. Wszystkie wydziały agencji posiadają też w niej własne strony internetowe, pozwalające zapoznać się z aktualnymi zadaniami, godzinami zebrań i narad, a także prezentacjami. Co noc całymi godzinami przeglądałem te zasoby.

Według Franka pierwsze zapytania, jakie wpisuje do wyszukiwarki wewnętrznej sieci agencji każdy nowo zatrudniony, dotyczą kosmitów i zamachów z 11 września. I właśnie dlatego, twierdził, nie można znaleźć w wynikach wyszukiwania żadnych sensownych informacji na żaden z tych tematów. Mimo to spróbowałem. Google CIA rzeczywiście nie znalazł niczego ciekawego, ale kto wie – być może prawda jest gdzieś tam… na jakimś innym dysku sieciowym. Dla porządku dodam jeszcze, że z tego, co mi wiadomo, kosmici nigdy nie nawiązali kontaktu z mieszkańcami Ziemi,

a w każdym razie nie skontaktowali się z amerykańskim wywiadem. Za to Al-Kaida utrzymywała bardzo bliskie relacje z naszymi sojusznikami Saudami – administracja Busha podejrzanie pilnie starała się ukryć informacje na ten temat w tym samym czasie, kiedy wyruszyliśmy na wojnę z dwoma innymi krajami.

CIA ani żaden z największych amerykańskich pracodawców, z wyjątkiem firm z Doliny Krzemowej, nie potrafili wówczas zrozumieć faktu, że spec od komputerów wie wszystko – albo raczej: jest w stanie dowiedzieć się wszystkiego. Im wyżej w hierarchii danej firmy lub organizacji się znajduje, im wyższe przywileje systemowe posiada, tym większy ma dostęp do każdego aspektu cyfrowej egzystencji swojego pracodawcy. Oczywiście nie każdy jest na tyle ciekawy, by zrobić użytek z tych możliwości, tak jak nie każdy, kto z nich korzysta, kieruje się wyłącznie czystą ciekawością. W moim wypadku buszowanie po systemach CIA było naturalnym przedłużeniem dziecięcego pragnienia, by zrozumieć, jak wszystko działa i jak różne elementy mechanizmu tworzą razem spójną całość. Stanowisko administratora systemu oraz związane z nim przywileje w połączeniu z biegłością techniczną pozwalały mi zaspokajać głód wiedzy i informacji. Gdyby was także to interesowało: tak, człowiek naprawdę wylądował na Księżycu. Zmiany klimatyczne zachodzą naprawdę. Smugi chemiczne to bzdura.

Na stronach wewnętrznego serwisu informacyjnego CIA czytałem ściśle tajne raporty i depesze na temat toczących się właśnie rozmów handlowych czy też zamachów stanu. Te relacje i opisy wydarzeń bardzo przypominały te, które kilka dni później pojawiały się w CNN czy Fox News. Najważniejsze różnice dotyczyły podawanych źródeł i szczegółowości informacji. O ile w gazecie czy w telewizji ograniczano się do stwierdzenia, że informacje o wstrząsach politycznych w danym kraju przekazał

„wysokiej rangi urzędnik, pragnący zachować anonimowość”, o tyle w wersji CIA podawano dokładnie, kto był źródłem informacji – na przykład „ZBSMACKTALK/1, pracownik ministerstwa spraw wewnętrznych, regularnie wykonujący powierzone mu zadania; posiada dostęp do informacji z drugiej ręki, które w przeszłości okazywały się wiarygodne”. Wystarczyło kilka kliknięć, żebym poznał prawdziwe nazwisko i uzyskał dostęp do pełnych akt osobowych ZBSMACKTALK/1.

Niektóre informacje, które znajdowałem w wewnętrznym serwisie informacyjnym, nigdy nie trafiały do mediów. Przez to jeszcze bardziej doceniałem znaczenie naszej pracy, a z drugiej strony miałem poczucie, że wiele mnie omija, ponieważ moja praca polega wyłącznie na siedzeniu przy stacji roboczej. Być może zabrzmi to nieco naiwnie, ale byłem szczerze zaskoczony, uświadomiwszy sobie, jak bardzo międzynarodowy charakter ma CIA – i nie chodzi mi wyłącznie o zasięg prowadzonych przez agencję operacji, ale także o jej kadry. To, jak wiele obcych języków słyszałem w naszej kantynie, wprawiało mnie w osłupienie. Uświadamiałem sobie wówczas swój prowincjonalizm. Praca w kwaterze głównej CIA była bez wątpienia ekscytująca, ale dzieliło mnie zaledwie kilka godzin jazdy samochodem od miejsca, w którym dorastałem – pod wieloma względami wciąż tkwiłem w tym samym otoczeniu i środowisku. Miałem dwadzieścia parę lat i nie licząc kilku pierwszych lat życia spędzonych w Karolinie Północnej, odbytych w dzieciństwie krótkich wycieczek do baz Straży Wybrzeża pod dowództwem mojego dziadka oraz paru tygodni służby wojskowej w Forcie Benning, nigdy tak naprawdę nie wyjechałem poza Beltway.

Czytając o wydarzeniach w Wagadugu, Kinszasie i innych egzotycznych miastach, których nie byłbym w stanie odnaleźć na mapie innej niż komputerowa, coraz bardziej utwierdzałem się w przekonaniu, że

dopóki jestem młody, powinienem służyć mojej ojczyźnie, robiąc coś naprawdę ważnego poza jej granicami. W przeciwnym razie, myślałem sobie, stanę się drugim Frankiem: będę siedział za coraz większymi biurkami, zarabiając coraz więcej pieniędzy, aż w końcu dotrę do takiego etapu, gdy będę potrzebny tylko po to, by obsługiwać jakiś przyszły odpowiednik maszyny z taśmą.

To wtedy zrobiłem coś, co wydawało się zupełnie nie do pomyślenia. Podjąłem starania o to, by zostać budżetowcem.

Wydaje mi się, że ta decyzja zaskoczyła moich przełożonych, ale jednocześnie im schlebiała, ponieważ w większości przypadków droga kariery wiodła w odwrotnym kierunku: to urzędnicy państwowi po wielu latach pracy dla rządu przechodzili w poszukiwaniu wyższej płacy do sektora prywatnego. Żaden początkujący pracownik kontraktowy z branży technicznej nie decydował się na przejście do sfery budżetowej i obniżkę wynagrodzenia. Dla mnie jednak zostanie budżetowcem było logicznym i sensownym rozwiązaniem: będą mi płacić za podróżowanie po świecie.

Miałem szczęście: okazało się, że w agencji jest wolny etat. Po dziewięciu miesiącach pracy w charakterze administratora systemu złożyłem wniosek o angaż na stanowisko specjalisty technicznego w zagranicznej placówce CIA. Podanie szybko doczekało się pozytywnego rozpatrzenia.

Mój ostatni dzień w kwaterze głównej był formalnością. Wypełniłem już wcześniej wszystkie niezbędne papiery i wymieniłem zielony identyfikator na niebieski. Czekało mnie już tylko kolejne szkolenie formacyjne – jako budżetowiec odbyłem je w eleganckiej sali konferencyjnej obok cukierni Dunkin’ Donuts. Tam też przeszedłem uświęcony rytuał, jakiego nie doświadczył żaden pracownik kontraktowy. Uniosłem dłoń i złożyłem przysięgę wierności – nie rządowi i nie agencji,

której byłem teraz etatowym pracownikiem, tylko Konstytucji Stanów Zjednoczonych. Uroczyście przysięgam strzec i bronić Konstytucji Stanów Zjednoczonych przed wszystkim wrogami w kraju i za granicą.

Następnego dnia wsiadłem do mojej starej, wiernej hondy civic i wyruszyłem w podróż w wiejskie rejony Wirginii. Żeby dostać się na wymarzoną placówkę zagraniczną, musiałem najpierw wrócić do szkoły – pierwszej, którą miałem naprawdę ukończyć.

---

* WASP (skrót od White Anglo-Saxon Protestants, biali Anglosasi wyznania protestanckiego) – określenie osoby należącej do elitarnej warstwy społeczeństwa amerykańskiego (przyp. tłum.).

14_Liczyhrabia_ze_Wzgórza|

Moim pierwszym zadaniem jako świeżo upieczonego funkcjonariusza rządowego było udać się do miasteczka Warrenton w stanie Wirginia i zakwaterować się w tamtejszym motelu należącym do sieci Comfort Inn. Głównym klientem tego smętnego przybytku był „Departament Stanu", czyli – mówiąc wprost – CIA. Był to najpodlejszy z podłych moteli w Warrenton i przypuszczalnie właśnie dlatego został wybrany przez agencję. Im mniej postronnych gości, tym mniejsze ryzyko, iż ktoś mógłby się zorientować, że motel pełnił funkcję prowizorycznego internatu dla kursantów Ośrodka Szkoleniowego Warrenton, czyli – jak nazywali go pracownicy – Wzgórza.

Kiedy się zameldowałem, recepcjonista pouczył mnie, żebym nie korzystał ze schodów, do których dostępu broniła policyjna taśma. Dostałem pokój na drugim piętrze głównego budynku, z widokiem na parking i należące do motelu dodatkowe pawilony. Moje nowe lokum było słabo oświetlone, w łazience panoszył się grzyb, a brudne dywany upstrzone były dziurami po papierosach – poprzedni lokatorzy najwyraźniej nie przejmowali się wiszącą na ścianie tabliczką z informacją o zakazie palenia. Sfatygowany materac pokrywały ciemnofioletowe plamy; miałem nadzieję, że to ślady po alkoholu. Mimo wszystko pokój przypadł mi do gustu – byłem wtedy jeszcze w wieku, kiedy mieszkanie w takich warunkach wydaje się romantyczne. Pierwszą, bezsenną noc przeleżałem na łóżku, gapiąc się na owady, które kłębiły się pod plafonem na suficie.

Odliczałem godziny do kontynentalnego śniadania, które serwowano gościom motelu.

Nazajutrz rano okazało się, że na kontynencie Warrenton pod pojęciem śniadania rozumie się małe pudełko płatków Froot Loops oraz kartonik skwaśniałego mleka.

Witamy w budżetówce.

Motel Comfort Inn, zwany przez nas Obozem Innternowania, miał być moim domem przez najbliższych sześć miesięcy. Dano nam do zrozumienia, że nie powinniśmy informować naszych bliskich, gdzie dokładnie przebywamy ani co robimy. Podporządkowałem się tym zaleceniom i ograniczyłem do minimum wyjazdy do Marylandu, a nawet telefoniczne rozmowy z Lindsay. Poza tym i tak nie miałem zbyt wielu okazji do telefonicznych pogaduszek. Wnoszenie prywatnych telefonów na teren ośrodka szkoleniowego było zakazane, ponieważ wszystkie prowadzone tam kursy objęto klauzulą tajności, a zajęcia trwały od rana do wieczora. Nasi instruktorzy dbali o to, żebyśmy nie mieli zbyt wiele czasu na tęsknotę za domem.

Najbardziej znanym centrum szkoleniowym CIA jest tak zwana Farma, znajdująca się na terenie bazy wojskowej Camp Peary. Jej sława wynika przede wszystkim z faktu, że jest to jedyny taki ośrodek, o którym piarowcy agencji mogą rozmawiać otwarcie z filmowcami z Hollywood. Wzgórze z kolei jest najbardziej tajemniczą ze wszystkich placówek, gdzie szkolą się pracownicy CIA. Połączone radiowo i światłowodowo z satelitarną stacją przekaźnikową w Brandy Station – częścią systemu infrastruktury pomocniczej Ośrodka Szkoleniowego Warrenton – Wzgórze stanowi serce sieci teletransmisyjnej CIA. Położone jest stosunkowo blisko Waszyngtonu, a zarazem na tyle daleko, by nie ucierpiało w razie ataku nuklearnego na stolicę USA. Nieowijający w bawełnę starzy wyjadacze z kadry ośrodka

powtarzali często, że CIA mogłaby funkcjonować pomimo utraty kwatery głównej, ale nie podniosłaby się po ciosie, jakim byłoby zniszczenie Warrenton. Zważywszy, że na terenie Wzgórza mieszczą się obecnie dwa ogromne centra przechowywania tajnych danych – w tworzeniu jednego z nich brałem później udział – jestem skłonny się z nimi zgodzić.

Jak nietrudno się domyślić, Wzgórze zawdzięcza nazwę usytuowaniu na szczycie rozległego wzniesienia. Cały teren otacza ogrodzenie na tyle niepozorne, by nie wzbudzać niepotrzebnego zainteresowania. Kiedy przyjechałem na szkolenie, na Wzgórze prowadziła tylko jedna droga. Za bramą wjazdową zaczynał się podjazd tak stromy, że kiedy temperatura spadała i nawierzchnia pokrywała się lodem, jadące pod górę samochody traciły przyczepność i zsuwały się z pochyłości.

Tuż za strzeżonym punktem kontrolnym mieści się nadgryziona zębem czasu siedziba centrum szkolenia łączności dla członków personelu dyplomatycznego. Ta należąca do Departamentu Stanu placówka nieprzypadkowo została usytuowana w tak widocznym miejscu. Pełni funkcję przykrywki dla pozostałych rodzajów działalności prowadzonych na Wzgórzu – postronny obserwator może odnieść wrażenie, że Wzgórze to nic innego jak miejsce szkolenia pracowników pionu telekomunikacyjnego amerykańskiej dyplomacji. Dalej, w głębi terenu, rozmieszczone są niskie, nieoznakowane budynki, gdzie odbywały się nasze zajęcia; jeszcze dalej znajduje się strzelnica, na której doskonalą umiejętności specjalni agenci wywiadu. Dobiegające stamtąd odgłosy wystrzałów rozbrzmiewały w nieznanym mi wcześniej rytmie: *pop-pop*, *pop*; *pop-pop*, *pop*. Dwa szybkie strzały służą obezwładnieniu przeciwnika; trzeci, starannie wymierzony oddaje się po to, by trwale go wyeliminować.

Na Wzgórze trafiłem jako uczestnik kursu numer 6-06 odbywającego się w ramach Programu Podstawowego Szkolenia Telekomunikacyjnego –

pod tą nudną nazwą kryje się jeden z najbardziej tajnych i niezwykłych programów szkoleniowych, jakie tylko istnieją. Jego celem jest zaspokajanie zapotrzebowania CIA na Specjalistów do spraw Bezpieczeństwa Teleinformatycznego (TISO, Technical Information Security Officers) – elitarną kadrę fachowców w dziedzinie łączności i komunikacji, zwanych potocznie *commo guys*. TISO ma być specem od wszystkiego, zdolnym pełnić w pojedynkę obowiązki, które w przeszłości spoczywały na szyfrantach, radiooperatorach, elektrykach, mechanikach, doradcach do spraw bezpieczeństwa fizycznego i cyfrowego, a także informatykach. Głównym zadaniem TISO jest obsługa infrastruktury technicznej umożliwiającej skuteczne prowadzenie operacji wywiadowczych CIA. Większość TISO pracuje pod przykrywką w zagranicznych bazach operacyjno-wywiadowczych agencji, będących najczęściej rezydenturami przy konsulatach i ambasadach Stanów Zjednoczonych – stąd też powiązania z Departamentem Stanu. Pracując w amerykańskiej placówce dyplomatycznej, czyli z dala od ojczyzny, w obcym kraju, którego mieszkańcom nie można ufać – dla CIA wszyscy obcokrajowcy są z zasady niegodni zaufania, niezależnie od tego, czy są obywatelami państwa wrogiego, czy sojuszniczego – musisz być samowystarczalny we wszystkich kwestiach dotyczących techniki i samodzielnie rozwiązywać wszelkie problemy. Jeśli powierzysz usunięcie usterki w swojej supertajnej bazie szpiegowskiej lokalnemu fachowcowi, to poradzi on sobie z tym bez trudu i być może zrobi to nawet całkiem tanio – ale przy okazji na polecenie służb wywiadowczych danego kraju naszpikuje twoją bazę trudnymi do wykrycia pluskwami.

Dlatego TISO musi umieć samodzielnie naprawić niemal każde urządzenie w budynku ambasady, począwszy od komputerów i sieci komputerowych przez systemy monitoringu wizyjnego, instalacje

grzewcze, wentylacyjne i klimatyzacyjne, czyli wszelkiego rodzaju panele słoneczne, grzejniki czy klimatyzatory, systemy zasilania awaryjnego i agregaty prądotwórcze, łącza satelitarne, wojskowe urządzenia szyfrujące aż po alarmy, zamki i tym podobne. Ogólna zasada jest taka, że TISO odpowiada za każde urządzenie posiadające wtyczkę oraz gniazdo, do którego można wpiąć wtyczkę.

TISO musi również wiedzieć, jak zbudować przynajmniej niektóre z wyżej wymienionych systemów, a także jak je zniszczyć – wiedza ta może się okazać niezbędna, jeśli placówka dyplomatyczna znajdzie się w stanie oblężenia i pojawi się ryzyko wtargnięcia na jej teren intruzów. W takiej sytuacji TISO zawsze opuszcza posterunek ostatni. Kiedy wszyscy dyplomaci i pozostali pracownicy agencji zostaną już ewakuowani, TISO wysyła do kwatery głównej CIA wiadomość z informacją o definitywnym zakończeniu łączności. Zanim jednak to zrobi, ma obowiązek podrzeć, spalić, skasować, rozmagnesować i rozbić w drobny mak wszystko, co w jakikolwiek sposób wiąże się z działalnością agencji. TISO musi zadbać o to, by żadne wartościowe informacje – w postaci dokumentów operacyjnych przechowywanych w sejfach ambasady albo zaszyfrowanych danych zapisanych na twardych dyskach – nie wpadły w ręce wroga.

O tym, że te wszystkie działania pozostają w gestii pracowników CIA, a nie urzędników Departamentu Stanu – choć przecież należą do niego wszystkie amerykańskie placówki dyplomatyczne – decyduje coś więcej niż tylko różnice kompetencji czy różny zakres odpowiedzialności obu tych instytucji: prawdziwym powodem jest zapewnienie Departamentowi Stanu możliwości wiarygodnego wyparcia się wiedzy na temat tych działań. Tajemnicą poliszynela jest fakt, że najważniejszą funkcją ambasad jest dziś zapewnianie zaplecza dla operacji wywiadowczych. Wraz z upowszechnieniem się elektronicznych środków komunikacji oraz

samolotów odrzutowych straciły na znaczeniu wszystkie dawne powody, dla których rządy państw utrzymywały oficjalne przedstawicielstwa na terenie innych krajów. Obecnie większość działań o charakterze dyplomatycznym odbywa się na szczeblu ministerialnym i w ramach bezpośrednich kontaktów między ministrami zainteresowanych państw. Oczywiście ambasady wciąż od czasu do czasu podejmują interwencje dyplomatyczne oraz służą pomocą przebywającym za granicą obywatelom danego kraju, a wydziały konsularne wydają wizy i przedłużają ważność paszportów. Urzędnicy konsularni rezydują jednak często w zupełnie innej siedzibie, a poza tym tego rodzaju działalność nie uzasadnia ogromnych wydatków ponoszonych na utrzymanie rozbudowanego aparatu zagranicznych reprezentacji. Natomiast da się uzasadnić te koszty możliwością wykorzystania infrastruktury dyplomatycznej jako przykrywki dla działań o charakterze szpiegowskim.

Pod taką przykrywką pracują między innymi TISO, którzy najczęściej formalnie pełnią funkcję rozmaitych attaché. W największych placówkach dyplomatycznych pracuje zwykle pięciu takich specjalistów; w nieco mniejszych ambasadach może być ich trzech, ale w większości na całą ambasadę przypada tylko jeden Specjalista do spraw Bezpieczeństwa Teleinformatycznego. Takich skazanych na samotne wykonywanie swoich obowiązków TISO określa się w agencji mianem singletonów. Zostaliśmy uprzedzeni, że ze wszystkich pracowników CIA to właśnie singletoni najczęściej się rozwodzą. Bycie samotnym specjalistą do spraw technicznych oznacza życie z dala od domu, w świecie, gdzie wszystko ciągle się psuje i nie ma nikogo, kto mógłby mu pomóc.

Wraz ze mną kurs numer 6-06 rozpoczęło siedmiu innych kursantów i tylko jeden z nas go nie ukończył – tak wysoki odsetek pomyślnie zakończonych szkoleń zdarza się podobno dość rzadko. Tworzyliśmy

barwną zbieraninę, a łączyło nas to, że każdy z nas miał w sobie niespokojnego ducha, który sprawiał, że byliśmy gotowi poświęcić znaczną część swojej kariery na tajną służbę w jakimś obcym kraju. Po raz pierwszy od rozpoczęcia pracy w agencji nie byłem najmłodszy w grupie. Miałem dwadzieścia cztery lata i pod względem wieku plasowałem się mniej więcej pośrodku stawki. Dzięki pracy na stanowisku administratora systemów w kwaterze głównej orientowałem się w działaniach agencji lepiej niż pozostali kursanci, z których większość stanowili zafascynowani nowoczesnymi technologiami, świeżo upieczeni absolwenci college'ów albo osoby prosto z ulicy, które trafiły na kurs po wypełnieniu formularza zgłoszeniowego w internecie.

Żeby uczynić zadość wojskowym obyczajom, jakim hołduje się w zagranicznych placówkach CIA, rzadko zwracaliśmy się do siebie po imieniu – znacznie częściej używaliśmy ksywek nawiązujących do aparycji, dziwactw albo faktów z życiorysu. Kolega, któremu nadaliśmy przezwisko Taco Bell, był typowym chłopakiem z przedmieścia, naiwnym, sympatycznym i niezbyt lotnym; miał dwadzieścia lat, a jego dotychczasowa kariera zawodowa ograniczała się do posady kierownika nocnej zmiany w barze Taco Bell w Pensylwanii. Dobiegający trzydziestki Rainman przez całe szkolenie przechodził autystyczne wahania nastroju, od stanów katatonicznej obojętności po napady furii. Z dumą przyjął nadane mu przezwisko i twierdził, że w indiańskiej tradycji Rainman to bardzo zaszczytne imię. Flet z kolei zawdzięczał ksywkę ukończeniu konserwatorium muzycznego ze specjalnością gry na fletni Pana; ten epizod z jego życia wydał się nam znacznie bardziej interesujący niż fakt, że Flet był weteranem piechoty morskiej. Trzydziestopięcioletni Spo zaliczał się do najstarszych kursantów. Jego przezwisko nawiązywało do funkcji, jaką pełnił wcześniej w CIA – był SPO (Special Police Officer), czyli

funkcjonariuszem straży ochrony obiektów agencji. Służba w wartowni przy bramie kwatery głównej w McLean nużyła go jednak do tego stopnia, że gotów był zrobić wszystko, byle tylko dostać się na placówkę zagraniczną. Ściągnął do Warrenton bliskich, którzy musieli gnieździć się wraz z nim w jednym motelowym pokoju (ostatecznie zmuszeni byli się wyprowadzić, ponieważ personel motelu natknął się na węża, którego dzieci Spo hodowały w szufladzie komody). Najstarszy z nas był Pułkownik, czterdziestokilkuletni były sierżant łączności Sił Specjalnych, który w trakcie służby wojskowej zaliczył kilka turnusów w piaskownicy*, a teraz poszukiwał nowej ścieżki kariery. Nazywaliśmy go Pułkownikiem, bo chociaż nie był oficerem, to aparycją przypominał pułkownika Sandersa z reklam Kentucky Fried Chicken (nawiasem mówiąc, smażone kurczaki z KFC stanowiły dla nas smakowitą odskocznię od potraw serwowanych w stołówce ośrodka w Warrenton).

W tym miejscu powinienem chyba wspomnieć o mojej ksywce. Koledzy ochrzcili mnie Liczyhrabią, ale nie skłoniły ich do tego moje arystokratyczne maniery ani dandysowski styl ubioru. Zostałem Liczyhrabią, bo kiedy w trakcie zajęć chciałem wtrącić swoje trzy grosze, wykonywałem identyczny gest, jak filcowy wampir z *Ulicy Sezamkowej* – unosiłem wskazujący palec, zupełnie jakbym miał zaraz zawołać: „Jedna, dwie, trzy, ha, ha, ha, trzy rzeczy, o których zapomniałeś!”.

Razem z kolegami uczestniczyłem w około dwudziestu cyklach zajęć przedmiotowych. Poświęcono je różnym zagadnieniom, ale większość krążyła wokół odpowiedzi na pytanie, jak najlepiej wykorzystać dostępne w konkretnych okolicznościach – czy to w ambasadzie, czy to w warunkach polowych – narzędzia i technologie i zaprząc je do pracy na rzecz rządu Stanów Zjednoczonych.

Jedno z ćwiczeń polegało na wtaszczeniu na dach budynku ważącej trzydzieści pięć kilogramów walizki, wypełnionej sprzętem łącznościowym, który wyprodukowano w czasach, gdy nie było mnie jeszcze na świecie. Mając do dyspozycji wyłącznie kompas i laminowaną tabelę współrzędnych, musiałem odnaleźć na nocnym niebie pośród mrowia migotliwych gwiazd jednego z tajnych satelitów CIA, który pozwoliłby mi nawiązać połączenie z naszym „statkiem-bazą", czyli z Centrum Łączności Kryzysowej CIA w McLean (sygnał wywoławczy „Centrala"). Następnie posługując się wyciągniętym z walizki nadajnikiem pamiętającym czasy zimnej wojny, zestawiłem zaszyfrowane łącze radiowe. Ćwiczenie to przypominało nam w praktyce, dlaczego specjalista do spraw łączności i komunikacji jest niezbędnym ogniwem każdej operacji CIA: szef placówki może wykraść wrogom ich najcenniejsze i najpilniej strzeżone tajemnice, ale nie będzie z nich żadnego pożytku, dopóki ktoś nie prześle ich do Ameryki.

Tamtej nocy zostałem w ośrodku dłużej i pojechałem samochodem na najwyżej położone miejsce na Wzgórzu: parking obok starej stajni przerobionej na salę wykładową, gdzie uczyliśmy się, jak zapobiegać monitorowaniu naszej elektronicznej aktywności przez naszych adwersarzy. Wiele metod, które tam poznawaliśmy, sprawiało wrażenie z pogranicza magii – jedna z nich, zwana phreakingiem Van Ecka, polega na podglądaniu z daleka obrazu wyświetlanego na ekranie dowolnego monitora komputerowego; jest to możliwe dzięki przechwytywaniu za pomocą specjalnej anteny pola elektromagnetycznego, emitowanego przez prądy oscylujące w obwodach komponentów monitora. Jeśli trudno ci to sobie wyobrazić, to nie martw się; zapewniam, że my również mieliśmy z tym problem. Nawet nasz instruktor przyznał bez ogródek, że nigdy nie był w stanie zrozumieć szczegółowych zasad tej metody i nie może

zademonstrować nam jej w działaniu. Zarazem był jednak przekonany, że zagrożenie jest jak najbardziej realne: CIA stosowała tę metodę do przechwytywania informacji, a zatem inni mogli wykorzystać ją przeciwko nam.

Wspiąłem się na dach mojego samochodu, białej wiekowej hondy civic. Kiedy usiadłem, poczułem się tak, jakbym miał stamtąd widok na całą Wirginię. Zadzwoniłem do Lindsay, po raz pierwszy od paru tygodni, a może nawet od miesiąca. Rozmawialiśmy, dopóki nie rozładowała się bateria w moim telefonie. Noc robiła się coraz chłodniejsza; mój oddech stał się widoczny, przybierając postać delikatnej mgiełki. Pragnąłem podzielić się z Lindsay panoramą, jaka roztaczała się ze szczytu Wzgórza – ciemnymi polami, pofałdowanymi wzniesieniami, rozgwieżdżonym niebem – ale musiałem ograniczyć się do odmalowania obrazu słowami. I tak zignorowałem już zasady, wnosząc na teren ośrodka telefon; zrobienie zdjęcia oznaczałoby złamanie prawa.

W programie szkolenia dużo uwagi poświęcano serwisowaniu terminali i kabli, czyli podstawowych – a pod wieloma względami także prymitywnych – komponentów infrastruktury telekomunikacyjnej każdej placówki CIA. „Terminal” w tym kontekście oznacza po prostu komputer, używany do wysyłania i odbierania wiadomości przekazywanych w obrębie jednej odpowiednio zabezpieczonej sieci. „Kable” w żargonie pracowników CIA to inaczej wiadomości, ale specjaliści do spraw technicznych wiedzą, że „kable” to także najzwyklejsze przedmioty: biegnące pod ziemią, a także po dnach mórz i oceanów przewody, które przez ostatnie półwiecze łączyły rozsiane po całym świecie terminale agencji, w tym zwłaszcza zabytkowe już dzisiaj terminale teleksowe.

Od naszego rocznika po raz ostatni wymagano biegłej znajomości zagadnień dotyczących konfiguracji sprzętowych terminali, obsługi wielu

pakietów oprogramowania, a także, rzecz jasna, okablowania. Zajmowanie się izolacją i powłokami kabli w dobie łączności bezprzewodowej wydawało się niektórym moim kolegom nieco dziwacznym pomysłem. Ale za każdym razem, gdy ktoś z nas wyraził głośno wątpliwości co do przydatności przekazywanej nam wiedzy o archaicznych technologiach, instruktorzy przypominali nam, że nasz rocznik był pierwszym w historii programu szkolenia TISO, który nie musiał uczyć się alfabetu Morse'a.

Kiedy zbliżał się termin zakończenia kursu, polecono nam wypełnić formularze; nazywaliśmy je listą marzeń. Otrzymaliśmy wykaz wszystkich placówek CIA, które cierpiały na braki kadrowe i mieliśmy uszeregować je w kolejności naszych preferencji. Wypełnione papiery trafiały do Działu Zapotrzebowania, gdzie od razu lądowały w koszu – a przynajmniej takie chodziły słuchy.

Na szczycie mojej listy znalazł się Dział Uzupełnień Specjalnych (Special Requirements Division, SRD). Formalnie rzecz biorąc, nie otrzymałbym przydziału do żadnej ambasady ani innej zagranicznej placówki, tylko do biura w Wirginii, skąd byłbym tymczasowo oddelegowywany do pracy w rozmaitych niezbyt przyjemnych zakątkach piaskownicy, gdzie służba była zbyt ciężka lub zbyt niebezpieczna, by agencja uznała za rozsądne skierować tam kogoś na stałe – mogły to być na przykład małe, wysunięte bazy operacyjne w Afganistanie, Iraku albo przygranicznych regionach Pakistanu. Wybrałem SRD, ponieważ liczyłem na urozmaiconą i pełną wyzwań służbę; nie uśmiechała mi się perspektywa spędzenia trzech lat w jednym i tym samym mieście. Moi instruktorzy z Warrenton byli przekonani, że SRD skwapliwie skorzysta z okazji, by mnie do siebie ściągnąć, a ja byłem przekonany, że znajdę tam pole do popisu dla moich świeżo nabytych umiejętności. Sprawy jednak potoczyły się inaczej, niż tego oczekiwałem.

Już sam fakt, że zakwaterowano nas w obskurnym motelu Comfort Inn świadczył o tym, że Ośrodek Szkoleniowy Warrenton stara się ciąć koszty. Z czasem niektórzy uczestnicy kursu 6-06 zaczęli nawet przebąkiwać, że kierownictwo ośrodka dopuszcza się łamania przepisów federalnego prawa pracy. Dla mnie – młodego pracoholika, który nie założył jeszcze rodziny – początkowo nie stanowiło to problemu. Podobnie było z innymi kursantami w moim wieku. Na tyle często padaliśmy ofiarą takiego drobnego wyzysku ze strony pracodawcy, że wydawało nam się to zupełnie normalne. Ale dla starszych niepłatne nadgodziny, brak urlopów i niewywiązywanie się przełożonych z wypłaty gwarantowanych przez prawo świadczeń rodzinnych stanowiły prawdziwy problem. Pułkownik musiał co miesiąc płacić alimenty, a Spo miał rodzinę: w ich sytuacji liczył się każdy dolar i każda minuta.

Wszystkie żale i pretensje wróciły ze zdwojoną siłą po tym, jak w naszym motelu zawaliły się zniszczałe schody. Na szczęście nikt nie ucierpiał, ale nie mogliśmy otrząsnąć się z szoku; moi koledzy zaczęli otwarcie mówić o tym, że gdyby CIA nie była głównym klientem Comfort Inn, to motel już dawno zostałby zamknięty z powodu niespełnionych norm przepisów przeciwpożarowych. Niezadowolenie zataczało coraz szersze kręgi i niewiele brakowało, by w szkole dla szpiegów powstał związek zawodowy. Kierownictwo ośrodka postanowiło wziąć nas na przeczekanie, wychodząc z założenia, że już wkrótce wszyscy wywrotowcy albo ukończą kurs i wyjadą na zagraniczne placówki, albo pożegnają się z pracą w agencji.

Kilku kolegów zwróciło się do mnie z pewną propozycją. Wiedzieli, że byłem lubiany przez instruktorów, bo osiągałem jedne z najlepszych wyników w naszej grupie. Wiedzieli również, że pracowałem wcześniej w kwaterze głównej i dzięki temu miałem większe pojęcie

o biurokratycznych procedurach obowiązujących w agencji. Poza tym całkiem nieźle radziłem sobie z pisaniem – przynajmniej jak na kogoś, kto na co dzień zajmował się techniką. Dlatego współkursanci poprosili mnie, żebym podjął się roli przedstawiciela uczestników kursu – albo zgodził się na męczeństwo – i formalnie przedstawił skargi dyrektorowi ośrodka.

Chciałbym móc powiedzieć, że podjąłem się tego zadania powodowany wyłącznie urażonym poczuciem sprawiedliwości. Z pewnością był to jeden z powodów, ale nie ukrywam, że dla młodego człowieka, który osiągał świetne wyniki we wszystkim, czego się podejmował, rzucenie wyzwania postępującemu nieuczciwie kierownictwu ośrodka okazało się też po prostu niezłą frajdą. Niespełna godzinę później przeglądałem zasoby wewnętrznej sieci agencji i wynotowywałem przepisy, na które zamierzałem się powołać. Jeszcze tego samego dnia wysłałem e-mail do dyrektora.

Nazajutrz rano dyrektor wezwał mnie do gabinetu. Przyznał, że ośrodek nie funkcjonuje idealnie, ale dodał, że rozwiązanie tych problemów przekracza jego możliwości.

– Zostało wam jeszcze tylko dwanaście tygodni. Bądź tak miły i powiedz kolegom, żeby wzięli się w garść i przemęczyli do końca kursu. Niedługo otrzymacie przydziały i będziecie mieć na głowie większe zmartwienia. A z całego pobytu tutaj zapamiętacie tylko to, kto otrzymał najlepszą ocenę końcową – powiedział.

Zrobił to w taki sposób, że jego słowa można było odczytać jako groźbę albo próbę przekupstwa. Tak czy inaczej, nie spodobało mi się to, co usłyszałem. Zabawa się skończyła – teraz chodziło mi już wyłącznie o to, by sprawiedliwości stało się zadość.

Moi koledzy zareagowali na informację o przegranej tak, jakby się jej spodziewali. Pamiętam, że kiedy Spo zauważył moje zmarszczone brwi, powiedział pocieszająco:

– Nie przejmuj się, stary. Przynajmniej spróbowałeś.

Spo pracował w agencji najdłużej z nas; wiedział, w jaki sposób funkcjonowała, i zdawał sobie sprawę, jak niedorzeczne było oczekiwanie, że kierownictwo naprawi coś, co samo wcześniej zepsuło. Ja tymczasem byłem rozgoryczony nie tylko porażką, ale i spokojem, z jakim Spo i pozostali przyjęli niepowodzenie. Nie chodziło o to, że moim kolegom nie zależało na rozwiązaniu problemu na tyle mocno, by gotowi byli o to walczyć – oni po prostu czuli, że nie mogą sobie na tę walkę pozwolić. System został zaprojektowany tak, by spodziewane koszty eskalacji konfliktu przewyższały potencjalne korzyści z odniesionego w nim zwycięstwa. W wieku dwudziestu czterech lat nie dbałem jednak ani o koszty, ani o korzyści. Interesowała mnie wyłącznie zmiana systemu. I nie zamierzałem składać broni.

Napisałem e-mail od nowa, wprowadzając kilka poprawek, po czym wysłałem go raz jeszcze – tym razem jednak nie do dyrektora ośrodka szkoleniowego, lecz do jego szefa: dyrektora Grupy Służby Terenowej. W hierarchii agencji stał on wyżej od dyrektora ośrodka w Warrenton, ale pod względem rangi i starszeństwa służbowego znajdował się na mniej więcej tym samym poziomie, co niektórzy dyrektorzy, z którymi miałem do czynienia w kwaterze głównej. Potem wysłałem kopię e-maila do jego szefa, który z całą pewnością przewyższał rangą każdego urzędnika agencji, z jakim się dotąd zetknąłem.

Kilka dni później nasza grupa uczestniczyła w zajęciach z kryptografii poświęconych prostym technikom szyfrowania w warunkach polowych, kiedy do sali weszła sekretarka dyrektora i ogłosiła koniec starego systemu. Niepłatne nadgodziny zostały zniesione, a za dwa tygodnie czekała nas przeprowadzka do znacznie lepszego hotelu. Pamiętam dumę, z jaką oznajmiła nam nazwę naszego nowego lokum: „Hampton Inn!”.

Upajałem się zwycięstwem tylko przez jeden dzień. Nazajutrz nasze zajęcia ponownie zostały przerwane: tym razem w drzwiach stanął sam dyrektor ośrodka i polecił mi udać się wraz z nim do jego gabinetu. Spo poderwał się z krzesła, objął mnie mocno, a potem udał, że ociera łzę, i zapewnił, że nigdy mnie nie zapomni. Zniecierpliwiony dyrektor wywrócił oczami.

W gabinecie czekał na nas dyrektor Grupy Służby Terenowej – przełożony dyrektora ośrodka, a także zwierzchnik niemal całej kadry specjalistów agencji do spraw łączności i telekomunikacji; szef, do czyjego szefa wysłałem kilka dni wcześniej e-mail. Przywitał się ze mną nad wyraz serdecznie i w przeciwieństwie do naszego dyrektora, który zaciskał gniewnie szczęki, nie przejawiał żadnej irytacji. Ten jego spokój wytrącił mnie z równowagi.

Starałem się nie dać po sobie poznać zdenerwowania, ale miałem wrażenie, jakbym pocił się od wewnątrz. Dyrektor ośrodka zaczął mówić o tym, że problemy, na jakie zwrócili uwagę uczestnicy naszego kursu, są obecnie rozwiązywane, ale jego przełożony szybko mu przerwał.

– Nie spotkaliśmy się tu po to, żeby rozmawiać o tych sprawach. Spotkaliśmy się, by porozmawiać o niesubordynacji i o hierarchii służbowej.

Byłbym mniej zaszokowany, gdyby dał mi w twarz.

Nie miałem pojęcia, jaką niesubordynację ma na myśli; zanim zdążyłem go o to zapytać, zaczął mówić o tym, że CIA różni się bardzo od innych cywilnych agencji, nawet jeśli różnicy tej nie widać na papierze. W agencji, która wykonuje tak ważne i odpowiedzialne zadania, przestrzeganie zasad hierarchii służbowej to sprawa kluczowa.

Uniosłem w górę palec wskazujący – zrobiłem to mimowolnie, ale w uprzejmy sposób – i przypomniałem, że zanim wysłałem e-maile do

wyższych rangą funkcjonariuszy agencji, próbowałem bezskutecznie załatwić sprawę u mojego bezpośredniego przełożonego. Była to ostatnia rzecz, jaką powinienem wyjaśniać owemu przełożonemu, który siedział przede mną po drugiej stronie biurka.

Dyrektor ośrodka wpatrywał się w czubki swoich butów, co jakiś czas rzucając spojrzenie w kierunku okna.

– Posłuchaj, Ed – zwrócił się do mnie jego szef. – Nie przyjechałem tu po to, żeby sporządzać raport o czyichś „zranionych uczuciach”. Spokojnie. Zdaję sobie sprawę, że zdolny z ciebie chłopak. Rozmawialiśmy o tobie z twoimi instruktorami i wszyscy byli zgodni, że masz talent i jesteś bystry. Zgłosiłeś się nawet na ochotnika do wyjazdu do strefy wojny. Doceniamy to. Chcemy, żebyś dla nas pracował, ale musimy mieć pewność, że możemy na ciebie liczyć. Musisz zrozumieć, że obowiązuje u nas pewien system. Czasem wszyscy musimy pogodzić się z czymś, co się nam nie podoba. Najważniejsze jest zadanie, które mamy do wykonania, a nie zdołamy go wykonać, jeśli każdy będzie podważał decyzje przełożonych.

Umilkł na chwilę, przełknął ślinę, po czym dodał:

– To szczególnie ważne na pustyni. Na pustyni dzieje się wiele różnych rzeczy, a ja nie mam na razie pewności, czy będziesz wiedział, jak sobie z nimi poradzić.

A więc na tym polegała ich zemsta. Dyrektor ośrodka uśmiechnął się pod nosem, spoglądając na parking za oknem. Nikt poza mną – ani jeden z pozostałych uczestników kursu – nie umieścił SRD ani żadnej placówki na terenach objętych działaniami wojennymi na pierwszym, drugim ani nawet na trzecim miejscu listy marzeń. Wszyscy poza mną wybierali placówki w Europie, w urokliwych miastach, gdzie można w spokoju popijać szampana, spoglądając na wiatraki i rowery, i gdzie rzadko słychać huk eksplozji.

Jakby na przekór przydzielili mnie właśnie do jednej z takich lokalizacji. Wysyłali mnie do Genewy. Ukarali mnie, dając mi coś, o co nigdy nie prosiłem i na czym zależało każdemu oprócz mnie.

Dyrektor Grupy Służby Terenowej wydawał się czytać w moich myślach, bo powiedział:

– To nie jest kara, Ed. To okazja, naprawdę. Ktoś z twoją wiedzą i umiejętnościami marnowałby się w strefie wojennej. Potrzebujesz większej placówki, takiej, gdzie wdraża się najnowsze rozwiązania. W tych warunkach nie będziesz się nudził i rozwiniesz skrzydła.

Wszyscy koledzy z kursu, którzy gratulowali mi otrzymanego przydziału, zaczęli później mi zazdrościć i uważali, że wysłano mnie do Genewy po to, żeby uniknąć kolejnych moich skarg. Siedząc w gabinecie dyrektora, pomyślałem sobie coś przeciwnego: podejrzewałem, że dyrektor miał wśród kursantów swojego informatora, który zdradził mu, jakiej placówki za wszelką cenę chciałem uniknąć.

Dyrektor Grupy Służby Terenowej wstał i uśmiechnął się. Spotkanie dobiegło końca.

– W porządku, a więc wszystko ustalone. Zanim wyjadę, chcę się jeszcze upewnić, czy na pewno dobrze się zrozumieliśmy. Nie będę miał już więcej problemów z Edem Snowdenem, prawda?

---

* Ang. *sandbox* – popularne wśród amerykańskich żołnierzy określenie pustynnych regionów Bliskiego Wschodu i Azji Południowej.

15_Genewa

Fabuła napisanego w 1818 roku *Frankensteina* Mary Shelley rozgrywa się w dużej części w Genewie – pełnym życia, zadbanym, czystym, działającym sprawnie niczym trybiki zegarka szwajcarskim mieście, które służyło mi teraz za dom. Jak wielu Amerykanów, dorastałem karmiony różnymi filmowymi, serialowymi i kreskówkowymi wersjami horroru Shelley, lecz nigdy nie miałem okazji zetknąć się z oryginałem. Z kolei gdy przeglądałem internetowe porady, co przeczytać na temat Genewy, niemal zawsze *Frankenstein* wyróżniał się na tle przewodników turystycznych i książek historycznych. W gruncie rzeczy, jeśli dobrze pamiętam, ściągnąłem sobie przed lotem tylko dwa PDF-y: właśnie *Frankensteina* (przeczytałem go w całości) i konwencje genewskie (ich nie przeczytałem). Na przestrzeni długich miesięcy, które spędziłem sam, zanim Lindsay przeprowadziła się do mnie, czytałem nocami wyciągnięty na materacu ułożonym w salonie absurdalnie ekskluzywnego i przestronnego, ale niemal zupełnie niewyposażonego apartamentu z widokiem na Rodan po jednej stronie i masyw gór Jura po drugiej. Ambasada wynajmowała to lokum przy Quai du Seujet w dzielnicy Saint-Jean Falaises.

Ograniczę się do stwierdzenia, że *Frankenstein* okazał się inny, niż sądziłem: ta powieść epistolarna przypominała w odbiorze ciąg rozwlekłych e-maili, a sceny szaleństwa i drastycznych morderstw przeplatały się w niej z przestrogami przed kosztem innowacji technologicznych często wyprzedzających przyjęte normy moralne, etyczne

i prawne. W książce prawidłowość ta prowadzi do powstania potwora, który wymyka się spod kontroli.

Temat tak zwanego efektu Frankensteina (znanego również pod zapożyczonym z wojska terminem *blowback*, czyli odrzut broni) przewija się często w kręgach wywiadowczych, głównie w kontekście decyzji politycznych, które – mimo że mają być działaniem w interesie narodowym Stanów Zjednoczonych – podkopują dobro kraju w sposób uniemożliwiający naprawę. Brzemienne w skutkach przykłady efektu Frankensteina przytaczane w cywilnych, rządowych, wojskowych, a nawet wywiadowczych analizach po fakcie obejmują szkolenie i finansowanie afgańskich mudżahedinów do walki z Sowietami, co poskutkowało radykalizacją Osamy bin Ladena i narodzinami Al-Kaidy, oraz wyrugowanie sympatyków partii Baas z armii Iraku po upadku Saddama Husajna, które to posunięcie doprowadziło do powstania Państwa Islamskiego. Natomiast najważniejszym przykładem efektu Frankensteina, z jakim zatknąłem się podczas mojej krótkiej kariery, były tajne działania rządu Stanów Zjednoczonych mające na celu restrukturyzację globalnych systemów łączności. W Genewie, w tej samej okolicy, gdzie szalał potwór Mary Shelley, Ameryka pieczołowicie budowała sieć, która z czasem zaczęła wieść samoistną, niezależną egzystencję i realizować własną misję, rujnując przy tym życie swoich twórców – w tym zdecydowanie również i moje.

Placówka CIA w ambasadzie amerykańskiej w Genewie była jednym z najważniejszych europejskich laboratoriów; to w niej od dziesięcioleci trwały prace nad tym właśnie eksperymentem. Los sprawił, że miasto będące wytworną siedzibą wielu banków należących do wpływowych rodzin i hołdujące odwiecznej tradycji dyskrecji znalazło się na

skrzyżowaniu międzynarodowej i europejskiej sieci światłowodowej oraz w zasięgu kluczowych satelitów telekomunikacyjnych.

CIA jest główną amerykańską agencją wywiadowczą skoncentrowaną na rozpoznaniu osobowym (HUMINT), czyli tajnym pozyskiwaniu informacji na drodze kontaktu interpersonalnego – osobistego, twarzą w twarz, bez pośrednictwa ekranu. Oficerowie prowadzący wyspecjalizowani w tej formie wywiadu są nieuleczalnymi cynikami i urzekającymi łgarzami; piją, palą i nie potrafią pogodzić się z rosnącym znaczeniem rozpoznania elektromagnetycznego (SIGINT), czyli tajnego pozyskiwania informacji wywiadowczych poprzez przechwyt danych z systemów łączności. SIGINT z każdym rokiem umniejszał ich przywileje i prestiż. Choć nie ufali technologii cyfrowej, przywodząc mi na myśl Franka z kwatery głównej, mieli pełną świadomość, że potrafi ona oddawać nieocenione usługi, co wzmagało produktywne poczucie koleżeństwa i zdrową rywalizację. Otóż nawet najbardziej przebiegły i charyzmatyczny oficer prowadzący przynajmniej kilkukrotnie w karierze trafia na zagorzałych idealistów, których lojalności nie da się kupić kopertą wypchaną banknotami. I wówczas zwykle zwraca się do jednego z oficerów technicznych, takich jak ja, z pytaniami, komplementami i zaproszeniami na imprezy.

Aby móc służyć jako oficer techniczny pośród tych ludzi, trzeba być w takim samym stopniu ambasadorem kulturalnym, co profesjonalnym doradcą; należało oswajać oficerów prowadzących z tradycjami i zwyczajami terytorium, które dla większości Amerykanów było równie obce, co Szwajcaria ze swoimi dwudziestoma sześcioma kantonami i czterema językami urzędowymi. W poniedziałek na przykład jeden z agentów mógł mieć do mnie prośbę o radę, jak przygotować tajny kanał łączności internetowej z potencjalnym zdrajcą, którego nie chciał spłoszyć.

We wtorek inny oficer przedstawiał mnie komuś, kogo nazywał specjalistą z Waszyngtonu – choć w rzeczywistości był to ten sam agent, co poprzedniego dnia, testujący przebranie, którego – wciąż wstyd mi to przyznać – nie spodziewałem się w najmniejszym nawet stopniu i zakładam, że taki był jego cel. W środę mogłem zostać zapytany o to, jak najskuteczniej zniszczyć dane po ich przetransmitowaniu (czyli dokonać informatycznej wersji spalenia po przeczytaniu) z dysku z informacjami o klientach, który oficerowi prowadzącemu udało się kupić od skorumpowanego pracownika Swisscomu. W czwartek mogło mnie czekać raportowanie naruszeń zasad bezpieczeństwa przez oficerów mojej komórki, na przykład tego, że nie zamknęli drzwi do swojej dziupli, wychodząc do ubikacji. Obowiązek ten wykonywałem z głębokim współczuciem, ponieważ kiedyś musiałem zaraportować sam siebie za popełnienie tego właśnie błędu. W piątek zaś mogło się zdarzyć, że poprosi mnie do swojego biura dyrektor operacyjny, żeby zapytać, czy gdyby – „hipotetycznie” – z centrali przysłano zainfekowany pendrive, a „ktoś” użyłby go do zhakowania komputerów używanych przez delegatów Organizacji Narodów Zjednoczonych (główny budynek ONZ znajdował się kawałek dalej przy naszej ulicy), to czy – moim zdaniem – istnieje duże niebezpieczeństwo, że taki „ktoś” zostałby złapany?

Moim zdaniem nie istniało. I nie został złapany.

Podsumowując: w okresie, który spędziłem w terenie, kształt działań agencji ulegał gwałtownym zmianom. CIA z coraz większą stanowczością oczekiwało od specjalistów rozpoznania osobowego, żeby dostosowali się do wyzwań nowego tysiąclecia, a od oficerów technicznych takich jak ja, by oprócz wykonywania wszystkich zwyczajnych obowiązków służyli im pomocą. My uczyliśmy ich tolerować sieć, a oni tolerowali nas.

Centrala postrzegała Genewę jako punkt zerowy tej transformacji, ponieważ to tu znajdowało się najgęstsze na świecie skupisko celów wysokiej jakości, obejmujące między innymi siedzibę główną Organizacji Narodów Zjednoczonych oraz centrale wielu jej wyspecjalizowanych agencji i różnych międzynarodowych organizacji pozarządowych. Mieściło się tu przedstawicielstwo Międzynarodowej Agencji Energii Atomowej działającej na rzecz techniki jądrowej i rozpowszechniającej standardy bezpieczeństwa, również te dotyczące broni nuklearnej; Międzynarodowy Związek Telekomunikacyjny, który – poprzez wpływ na normy techniczne obowiązujące w najróżniejszych dziedzinach od spektrum radiowego po orbity satelitów – określał, co i jak można transmitować; oraz Światowa Organizacja Handlu, ta – regulując wymianę dóbr, usług i własności intelektualnej między państwami członkowskimi – decydowała o tym, co i w jaki sposób wolno sprzedawać. Nie można było również pominąć roli Genewy jako finansowej stolicy sektora prywatnego – tutejsze banki umożliwiały przechowywanie i wydawanie ogromnych sum w tajemnicy przed publiką, niezależnie od legalności pochodzenia.

Znane z powolnego działania i przesadnej drobiazgowości tradycyjne techniki wywiadowcze zapewniły szereg niepodważalnych sukcesów w manipulowaniu genewskimi systemami na korzyść Stanów. Było to jednak zbyt mało, by zaspokoić nieustannie rosnący apetyt amerykańskich decydentów czytających raporty z działań wywiadu – tym bardziej od czasu, kiedy szwajcarski sektor bankowy, podobnie jak reszta świata bankowości, rozpoczął cyfryzację. Skoro największe tajemnice świata trafiły na dyski komputerów, a większość z nich łączyła się z ogólnodostępnym internetem, logiczne było, że amerykańskie siły wywiadowcze będą chciały wykorzystać tę nową drogę dostępu, by tajemnice te wykraść.

W erze przedinternetowej, aby zdobyć dane z upatrzonego komputera, należało pozyskać informatora z fizycznym dostępem do celu. Wymagało to złożenia takiej osobie propozycji obarczonej oczywistym ryzykiem: mogła przecież zostać przyłapana na zgrywaniu tajnych danych lub instalowaniu złośliwego sprzętu i oprogramowania mającego przesłać dane oficerowi prowadzącemu. Globalny rozwój technologii cyfrowej niesamowicie uprościł ten proces. W naszym nowym świecie, który umożliwia „pozyskiwanie danych z sieci cyfrowych" i „działania wywiadowcze w sieciach komputerowych", fizyczny dostęp do komputera prawie nigdy nie jest potrzebny. Tym samym ograniczono ryzyko grożące zamieszanym osobom i permanentnie zmieniono bilans sił pomiędzy przedstawicielami wywiadu osobowego i elektromagnetycznego. Agent może dziś po prostu wysłać celowi wiadomość, na przykład e-mail, z załącznikami instalującymi złośliwe oprogramowanie, które potrafi przejrzeć nie tylko dany komputer, ale i całą dostępną mu sieć.

Takie innowacje miały sprawić, że sekcja HUMINT Centralnej Agencji Wywiadowczej skupi się na rozpoznawaniu wartościowych celów, a SIGINT zajmie się resztą. Zamiast urabiać cel tak, by przeistoczyć go w informatora – przez położenie koperty na stół albo, jeśli przekupstwo nie poskutkuje, przez przymus i szantaż – można było osiągnąć podobny efekt za pośrednictwem kilku zmyślnych hakerskich sztuczek. Co więcej, dzięki zastosowaniu tej metody cel pozostawał nieświadomy swojego udziału, co naturalnie redukowało liczbę skutków ubocznych.

Na to w każdym razie liczono. Rzecz w tym, że w miarę przeistaczania się wywiadu w cyberwywiad (termin stosowany, by odróżnić rozpoznanie internetowe od starego SIGINT-u skoncentrowanego na telefonach i faksach) dawne zmartwienia wróciły pod zmienioną przez nowe medium

postacią. Pojawiły się takie problemy jak chociażby ten: w jaki sposób zbadać cel w sieci, nie ujawniając swojej tożsamości?

Kłopot ten zwykle występował wówczas, gdy oficer prowadzący wyszukiwał w bazach danych agencji nazwisko obywatela takich krajów jak Irak lub Chiny i nie otrzymywał odpowiedzi. „Brak wyników” był stosunkowo częstym komunikatem zwrotnym przy próbach zdobycia informacji o potencjalnym celu; bazy danych CIA zawierały przede wszystkim informacje o osobach, które już stanowiły obiekt zainteresowania agencji albo mieszkały w krajach zaprzyjaźnionych, skąd łatwiej było pozyskać potrzebne źródła. Agentowi postawionemu w takiej sytuacji pozostawało to samo, co tobie, kiedy próbujesz się czegoś o kimś dowiedzieć: zasięgnąć informacji w ogólnodostępnych zasobach internetu. Jest to jednak ryzykowne.

Zwykle kiedy wchodzisz do sieci, twój komputer wysyła żądanie dostępu do serwera, gdzie mieści się strona, którą chciałbyś odwiedzić. Rzecz w tym, że choć zapytanie podróżuje w zasadzie bezpośrednio do celu, po drodze mija szereg przystanków, na każdym radośnie oznajmiając, skąd dokładnie pochodzi i dokąd konkretnie zmierza. Dzieje się tak za sprawą nagłówków zawierających adres źródłowy i docelowy komunikatu, które stanowią odpowiednik adresu nadawcy i pola adresowego na pocztówce. Nagłówki te sprawiają, że wiele osób, między innymi zarządcy stron internetowych, administratorzy sieci i agenci wywiadu innych krajów, może bardzo łatwo rozpoznać, że te działania w sieci podejmowałeś ty, a nie kto inny.

Być może trudno w to uwierzyć, ale w tamtych czasach CIA nie miało dobrej odpowiedzi na pytanie, co powinien zrobić oficer prowadzący, który napotka taką trudność, poza sugerowaniem – bez przekonania – by poprosił centralę o wyszukanie danej osoby za niego. Była to absurdalna procedura,

od strony formalnej mająca działać w ten sposób, że ktoś w centrali w McLean wchodził do internetu ze specjalnego terminala komputerowego wykorzystującego tak zwany anonimizujący system zbierania informacji, skonfigurowany w taki sposób, by zapytanie przed trafieniem do Google'a przechodziło przez serwer proxy, co fałszowało jego pochodzenie. Gdyby ktokolwiek próbował dochodzić, kto wysłał dane żądanie, trafiłby na nijaką spółkę ulokowaną gdzieś w Stanach Zjednoczonych – jedną z dziesiątek firm headhunterskich i human resources, które służyły za przykrywki CIA.

Nikt nigdy nie wyjaśnił mi jednoznacznie, dlaczego CIA miała w zwyczaju wykorzystywać jako przykrywkę rożnego rodzaju agencje pośrednictwa pracy. Podejrzewam, że takie firmy jako jedyne nie wzbudzały niczyjego zainteresowania tym, że jednego dnia szukały w internecie inżyniera technik jądrowych z Pakistanu, a drugiego – emerytowanego polskiego generała. Jestem jednak w pełni przekonany, że metoda ta była nieskuteczna, uciążliwa i kosztowna. Stworzenie jednego takiego przykrywkowego przedsiębiorstwa wymagało wymyślenia dla niego konkretnej działalności gospodarczej i nazwy, zdobycia wiarygodnego fizycznego adresu na terenie Stanów, zarejestrowania autentycznej domeny internetowej, przygotowania rzetelnej strony i wynajęcia serwera, a następnie skonfigurowania szyfrowanego połączenia, które umożliwiało niepostrzeżone przesyłanie danych pomiędzy tymże serwerem a siecią agencji wywiadowczej. Wysiłek i wydatek włożone w zapewnienie nam możliwości anonimowego googlowania nazwisk szły niestety na marne z chwilą, gdy któryś z analityków postanowił się rozerwać i wchodził z tego samego komputera, na którym prowadził rozpoznanie, na swój facebookowy profil. To wystarczyło, by spalić przykrywkę – to znaczy ujawnić naszym wrogom powiązanie z CIA. Mało który z pracowników siedziby głównej działał bowiem pod przykryciem,

a profile facebookowe reszty dumnie oznajmiały: „Pracuję dla CIA” albo – z identycznym skutkiem – „Pracuję dla Departamentu Stanu, ale w McLean”.

Możesz się z tego śmiać, proszę bardzo, ale w tamtych czasach takie rzeczy zdarzały się cały czas.

Podczas mojego pobytu w Genewie za każdym razem, gdy któryś z oficerów prowadzących pytał mnie, czy istnieje bezpieczniejszy, szybszy i ogólnie bardziej wydajny sposób radzenia sobie z tym problemem, zapoznawałem ich z Torem.

Projekt Tor to dzieło rządu amerykańskiego, które stało się jedną z najskuteczniejszych osłon przed rządowym szpiegowaniem. Jest to darmowe oprogramowanie open source; starannie używane, pozwala przeglądać internet na tyle anonimowo, na ile jest to możliwe w dużej skali. Protokoły Tora powstały w Ośrodku Badawczym Marynarki Wojennej Stanów Zjednoczonych w połowie lat dziewięćdziesiątych XX wieku, a w 2003 roku zostały upublicznione – dostęp do nich zyskali cywile na całym świecie i to od tych użytkowników zależy obecnie ich skuteczność. Tor działa bowiem w oparciu o model społecznościowej współpracy, w którym kluczową rolę odgrywają komputerowo uzdolnieni ochotnicy z całego globu, utrzymujący na swoich strychach, w piwnicach i w garażach serwery Tora. To przez nie Tor przekierowuje ruch internetowy, chroniąc informacje o pochodzeniu pakietów podobnie jak anonimowy system CIA, z tą zasadniczą różnicą, że robi to lepiej, a w każdym razie skuteczniej. Mnie nie trzeba było przekonywać, w przeciwieństwie do zrzędliwych agentów starszej daty.

W protokole Tor ruch internetowy odbywa się losowo generowanymi ścieżkami pomiędzy serwerami. Celem tego rozwiązania jest to, żeby w komunikacji nie figurowała twoja sieciowa tożsamość, lecz adres

ostatniego serwera Tor w łańcuchu, którego ogniwa nieustannie zamieniają się miejscami. Praktycznie żaden z tych serwerów, nazywanych warstwami albo węzłami, nie zna tej tożsamości ani nie posiada informacji umożliwiających namierzenie źródła transmisji. A co najgenialniejsze, jedyny serwer, który wie, skąd nadeszła wiadomość – czyli pierwszy w łańcuchu – nie ma pojęcia, dokąd ona zmierza. Mówiąc prościej: pierwszy serwer Tora łączący cię z jego siecią, nazywany bramą, wie, że to ty wysłałeś zapytanie, ale ponieważ nie posiada pozwolenia, by przeczytać jego treść, nie ma też pojęcia, czy szukasz memów ze zwierzątkami, czy informacji o proteście; tymczasem ostatni serwer, przez który przepływa twoja transmisja, nazywany wyjściem, wie dokładnie, czego dotyczy pytanie, ale nie ma pojęcia, kto je zadał.

Ta wielowarstwowa technika przesyłania wiadomości nazywa się trasowaniem cebulowym i to od niej Tor bierze swoją nazwę: The Onion Router (router cebulowy). Dowcip z gatunku hermetycznych głosił, że prowadzenie rozpoznania w sieci Tor doprowadza szpiegów do płaczu. Na tym polega ironia tego przedsięwzięcia: mamy do czynienia z technologią opracowaną przez marynarkę Stanów Zjednoczonych, która uczyniła cyberwywiad trudniejszym i łatwiejszym jednocześnie – wykorzystała wiedzę hakerów do ochrony anonimowości oficerów sił wywiadowczych, ale za cenę zapewnienia tej samej anonimowości wrogom i zwyczajnym użytkownikom z całego świata. W tym sensie Tor był neutralny nawet bardziej niż Szwajcaria. Gdy go odkryłem, w moim życiu zaszła wielka zmiana, bo pozwolił mi cieszyć się internetem znanym z dzieciństwa. Dał mi namiastkę wolności od bycia obserwowanym.

Napisałem tu o rosnącym zainteresowaniu CIA cyberwywiadem (SIGINT-em w internecie), ale w żadnym razie nie chcę sugerować, że agencja

przestała prowadzić szeroko zakrojone rozpoznanie osobowe (HUMINT), którym zajmuje się od zawsze, a w każdym razie od chwili narodzin nowoczesnego wywiadu po drugiej wojnie światowej. Nawet ja się w to zaangażowałem, choć moja pamiętna operacja skończyła się porażką. Genewa była pierwszym i ostatnim miejscem w mojej karierze wywiadowczej, gdzie nawiązałem osobistą znajomość z celem – to tu pierwszy i ostatni raz spojrzałem inwigilowanemu prosto w oczy zamiast rejestrować jego życie z bezpiecznej odległości. Nigdy nie zapomnę tego przeżycia; było w nim coś przerażająco bezpośredniego i smutnego. Zdecydowanie łatwiej pod względem psychologicznym jest siedzieć i dyskutować o hakowaniu nieposiadającego twarzy kompleksu ONZ. Pośród techników wywiadu, a już w szczególności wśród informatyków, na ogół nie dochodzi do potencjalnie nieprzyjemnego i emocjonalnie wyczerpującego bezpośredniego kontaktu z celami. Separacja zapewniana przez ekran sprawia, że praca oficera technicznego jest wyraźnie bezosobowa. Obserwując życie innych przez okno monitora, prędzej czy później zaczyna się postrzegać swoje działania jako abstrakcyjne, co ogranicza zdolność do rzeczowego mierzenia się ze skutkami takich posunięć.

Mężczyznę, o którym będzie ta historia, poznałem na przyjęciu w ambasadzie. Ambasada organizowała takie imprezy bardzo często, a agenci pojawiali się na każdej z nich, kuszeni w tym samym stopniu okazją do wypatrzenia i oceny potencjalnych kandydatów na informatorów, co otwartym barem i palarnią cygar.

Czasami zabierali mnie ze sobą. Sądzę, że nasłuchali się ode mnie tyle o mojej dziedzinie, że nie mogli się doczekać, by nauczyć mnie czegoś więcej o swojej. Chcieli zapewne wyszkolić mnie tak, bym był w stanie pomóc im w znajdowaniu celów w tłumie, gdzie nie dawali rady sprawdzić

wszystkich. Moja ewidentna aparycja geeka sprawiała, że potrafiłem wywołać u młodych badaczy z CERN-u (Conseil européen pour la recherche nucléaire, Europejskiej Organizacji Badań Jądrowych) pełen ekscytacji słowotok; nie umieli tego magistrowie zarządzania i politologowie, którymi obsadzano bardziej tradycyjne stanowiska CIA.

Mnie, osobie zajmującej się sprawami technicznymi, było niezwykle łatwo chronić swoją przykrywkę. Kiedy tylko jakiś kosmopolita w garniturze szytym na miarę pytał mnie, czym się zajmuję, odpowiadałem dwoma słowami: „Jestem informatykiem" (albo – w moim coraz lepszym francuskim – czterema: „*Je travaille dans l'informatique*"). To wystarczało, by natychmiast tracił zainteresowanie moją osobą. Nie zdarzyło się jednak, by to oznaczało koniec rozmowy. Jako świeżo upieczony specjalista w rozmowie z przedstawicielem innej dziedziny nie budziłem podejrzeń, mimo że zadawałem wiele pytań. Doświadczenie zaś nauczyło mnie, że ludzie rzadko przepuszczają okazję, by wyjaśnić ze szczegółami, o ile więcej od ciebie wiedzą o tym, co jest dla nich bardzo ważne.

Utkwiła mi w pamięci zwłaszcza jedna impreza. Odbyła się w ciepłą noc na tarasie ekskluzywnej kawiarni przy jednej z bocznych uliczek na nabrzeżu Jeziora Genewskiego. Niektórzy agenci bez wahania porzucali mnie na tego rodzaju zbiegowiskach, jeśli zmuszała ich do tego konieczność zajęcia miejsca jak najbliżej kobiety spełniającej ich wyżyłowane kryteria celu wywiadowczego (takie jak wyjątkowa uroda i wiek studentki), ale nie narzekałem. Traktowałem wypatrywanie potencjalnych informatorów jak hobby z bonusem w postaci darmowej kolacji.

Wziąłem talerz i przysiadłem się do dobrze ubranego mężczyzny z Bliskiego Wschodu w demonstracyjnie szwajcarskiej różowej koszuli ze spinkami do mankietów. Sprawiał wrażenie samotnego i wyraźnie

poirytowanego tym, że nikt nie jest nim zainteresowany, więc poprosiłem, żeby opowiedział mi o sobie. To najczęściej stosowana technika: wykazujesz zainteresowanie i pozwalasz mówić. W tym wypadku mój nowy znajomy mówił tak wiele, że odniosłem wrażenie, jakby zapomniał o moim istnieniu. Pochodził z Arabii Saudyjskiej, zakochał się w Genewie, urzekło go piękno języka francuskiego w porównaniu z arabskim oraz uroda pewnej Szwajcarki, z którą regularnie spotykał się – tak! – na laserowym paintballu. Następnie, przyjmując nieco konspiracyjny ton, poinformował mnie, że zajmuje się zarządzaniem prywatnymi majątkami. Chwilę później słuchałem potoczystej, dopracowanej w szczegółach prezentacji na temat tego, co dokładnie czyni prywatny bank prywatnym i jakie wyzwania stoją przed inwestorem, który chce pozostać na jednym rynku, chociaż jego klienci są wielkości państwowych funduszy majątkowych.

– Pana klienci? – spytałem.

Wtedy odpowiedział:

– Pracuję głównie z klientami z Arabii Saudyjskiej.

Kilka minut później przeprosiłem go i poszedłem do łazienki. Mijając agenta zajmującego się celami ze świata finansów, nachyliłem się i wyjaśniłem, czego się dowiedziałem. Po odpowiednio długim czasie spędzonym na poprawianiu fryzury, to znaczy staniu przed lustrem i esemesowaniu z Lindsay, wróciłem na salę, gdzie oficer, któremu szepnąłem o bankowcu, siedział już na moim krześle. Pomachałem nowemu saudyjskiemu znajomemu i przysiadłem się do porzuconej przez agenta kobiety o oczach mocno podkreślonych cieniem do powiek. Nie było mi przykro – jeśli już, to miałem wrażenie, że naprawdę zasłużyłem na czekoladowe trufle Pavés De Genève, które zaczęły krążyć między gośćmi. Wykonałem swoje zadanie.

Nazajutrz oficer z poprzedniego wieczoru, nazwę go Cal, obsypał mnie pochwałami i podziękowaniami. Skuteczność pozyskiwania informatorów z dostępem do danych wartych formalnego zgłoszenia do centrali jest dla agenta wywiadu osobowego kluczowa. To ona decyduje o możliwości jego awansu. Zważywszy na podejrzenia wobec Arabii Saudyjskiej o finansowanie terrorystów, Cal odczuwał ogromną presję, by zwerbować dobrej jakości źródło. Byłem przekonany, że nasz wspólny znajomy z przyjęcia błyskawicznie zacznie otrzymywać od CIA drugą pensję.

Sprawy potoczyły się jednak inaczej. Mimo regularnych wyjść na drinki i do barów ze striptizem Cal nie zaskarbił sobie przyjaźni bankowca – ich relacja nie przeszła na taki etap, kiedy mógłby zaproponować mu współpracę. To zaś sprawiło, że Cal zaczął się niecierpliwić.

Po miesiącu nieskutecznych wysiłków jego frustracja osiągnęła taki poziom, że zabrał naszego wspólnego znajomego do baru, upił go prawie do nieprzytomności, a następnie namówił, żeby zamiast wziąć taksówkę, wrócił do domu własnym samochodem. Cal nie zaczekał nawet, aż facet ruszy spod ostatniego lokalu, który odwiedzili tego wieczora, i od razu zadzwonił z donosem na policję, a ta kwadrans później aresztowała Saudyjczyka za jazdę pod wpływem alkoholu. Oznaczało to dla niego ogromny mandat – w Szwajcarii kary pieniężne nie są z góry przyjętymi sumami, ustala się je w odniesieniu do zarobków – i zawieszenie prawa jazdy na trzy miesiące. Przez ten czas Cal, cudowny przyjaciel z udawanym poczuciem winy, woził swoją ofiarę z domu do pracy i z powrotem, żeby „nikt z firmy nie dowiedział się, co się stało”. Kiedy administracja wyegzekwowała mandat, przez co nasz wspólny znajomy zaczął mieć kłopoty z płynnością finansową, Cal już czekał z propozycją pożyczki. Bankier stał się od niego zależny, co było marzeniem każdego oficera prowadzącego.

Pojawił się tylko jeden szkopuł: kiedy Cal wreszcie zaproponował naszemu znajomemu współpracę, ten wpadł w furię. Domyślił się, że Cal wmanewrował go w popełnienie przestępstwa i aresztowanie, a nieszczerą wspaniałomyślność z jego strony uznał za osobistą zdradę. Zerwał z nim wszelkie kontakty. Cal próbował bez większych nadziei odnowić znajomość i ograniczyć szkody, ale było już na to za późno. Bankier, który tak pokochał Szwajcarię, stracił pracę i zaczął szykować się do powrotu – być może przymusowego – do Arabii Saudyjskiej. Cal zaś w następnej turze wrócił do Stanów.

Zbyt wiele zaryzykowaliśmy, za mało zyskaliśmy. Działania, które sam zainicjowałem, a później nie potrafiłem ich przerwać, przyniosły same straty. Po tym doświadczeniu zacząłem jeszcze lepiej rozumieć, dlaczego CIA odchodziło od wywiadu osobowego na rzecz elektronicznego.

Latem 2008 roku w mieście odbył się coroczny, pełen rozmachu festiwal Fêtes de Genève. Jego kulminacją jest zawsze pokaz fajerwerków. Pamiętam, że siedziałem gdzieś przy południowym brzegu Jeziora Genewskiego w towarzystwie pracowników genewskiej komórki Special Collection Service (SCS) – wspólnego programu CIA i NSA, polegającego na instalowaniu i obsadzaniu specjalistycznego sprzętu wywiadowczego, umożliwiającego ambasadom Stanów Zjednoczonych szpiegowanie łączności innych krajów.

Ludzie z SCS pracowali w ambasadzie przy tym samym korytarzu, przy którym mieściło się moje stanowisko, ale wszyscy byli starsi ode mnie, a zajęcie, które wykonywali, o wiele bardziej odpowiedzialne. Nie mówię już nawet o tym, że zupełnie przerastało moje umiejętności – NSA miało dostęp do narzędzi, z których istnienia zupełnie nie zdawałem sobie sprawy. Mimo to utrzymywaliśmy przyjazne stosunki: ja ich podziwiałem, a oni o mnie dbali.

Kiedy opowiedziałem przy akompaniamencie wybuchających na niebie fajerwerków o sprawie tamtego bankowca, ubolewając, że skończyła się taką katastrofą, jeden z ludzi SCS zwrócił się do mnie i doradził:

– Ed, kiedy następnym razem kogoś takiego spotkasz, nie trać czasu na agentów; po prostu daj nam jego e-mail, a my się wszystkim zajmiemy.

Pamiętam, że słysząc to, posępnie pokiwałem głową, choć wtedy praktycznie nie miałem pojęcia, co w rzeczywistości kryje się za tą wypowiedzią.

Do końca roku trzymałem się z dala od imprez. Spędzałem wolny czas w kawiarenkach i parkach Saint-Jean Falaises z Lindsay, z którą od czasu do czasu wyjeżdżałem na wakacje do Włoch, Francji i Hiszpanii. Mimo to coś psuło mi nastrój. Nie miało to związku wyłącznie z tamtą porażką, a kiedy teraz o tym myślę, być może chodziło nie o tego jednego bankowca, lecz o bankowość ogółem. Genewa to drogie miasto, nie wstydzi się swoich luksusów, ale pod koniec 2008 roku jej elegancja zaczęła mieć coraz więcej wspólnego z ekstrawagancją. Stało się tak za sprawą ogromnej fali superbogaczy – w większości obywateli krajów Zatoki Perskiej, przede wszystkim Arabii Saudyjskiej – korzystających w okresie poprzedzającym globalny kryzys finansowy ze szczytowych cen ropy naftowej. Wszyscy ci szejkowie i im podobni wynajmowali całe piętra pięciogwiazdkowych hoteli i ogołacali półki ekskluzywnych sklepów po drugiej stronie mostu widocznego z okien mojego mieszkania. Urządzali wystawne bankiety w restauracjach z rekomendacją Michelina i pędzili po brukowanych ulicach w chromowanych lamborghini. Ostentacyjna konsumpcja jest co prawda jednym ze znaków rozpoznawczych Genewy, ale w tamtym okresie rozrzutność bogaczy naprawdę kłuła w oczy – obserwowałem ją bowiem podczas załamania gospodarczego, które amerykańskie media nazywały

najgorszym od czasów wielkiego kryzysu, a europejskie – od czasów dwudziestolecia wojennego.

Nie chodziło o to, że nie starczało nam z Lindsay pieniędzy – nasz czynsz opłacał przecież Wujek Sam – lecz o to, że sytuacja naszych bliskich mieszkających w Stanach, z którymi regularnie rozmawialiśmy, robiła się coraz bardziej niewesoła. I moja rodzina, i krewni Lindsay, znali takich, co przepracowali całe życie, niektórzy nawet dla rządu Stanów Zjednoczonych, a bank odebrał im dom, kiedy nieoczekiwana choroba sprawiła, że przez kilka miesięcy nie było ich stać na spłatę rat kredytu hipotecznego.

Mieszkanie w Genewie przypominało przebywanie w alternatywnej, a nawet – można by rzec – przeciwstawnej rzeczywistości. Podczas gdy reszta świata biedniała, Genewa kwitła, a szwajcarskie banki, mimo że raczej nie uczestniczyły w ryzykownych transakcjach z rodzaju tych, które wywołały kryzys, bez skrupułów ukrywały pieniądze zyskane na cierpieniu innych przez tych, co ostatecznie uniknęli odpowiedzialności. Kryzys z roku 2008 sprawił, że wezbrała fala populizmu, która dziesięć lat później przetoczyła się przez Europę i Amerykę, i pomógł mi pojąć, że zdarzenia o niszczycielskich skutkach społecznych często okazują się korzystne dla elit. Wyciągnąłem z tej lekcji wnioski, a rząd Stanów Zjednoczonych na przestrzeni kolejnych lat na różne sposoby mnie w nich utwierdzał.

16_Tokio|

Internet jest z gruntu amerykański, ale musiałem wyjechać z Ameryki, by w pełni zrozumieć, co to znaczy. Sieć WWW wynaleziono co prawda w Genewie w 1989 roku w laboratoriach badawczych CERN-u, ale metody łączenia się z nią są tak amerykańskie jak baseball. Służby wywiadowcze Stanów Zjednoczonych cieszą się zatem przewagą wynikającą stąd, że podejmują szpiegów innych państw na własnym boisku. Tak ogromna większość infrastruktury – okablowania, satelitów, serwerów i nadajników – znajduje się pod kontrolą USA, że dziewięćdziesiąt procent światowego ruchu internetowego odbywa się za pośrednictwem amerykańskich technologii i urządzeń; są zaprojektowane i obsługiwane przez amerykański rząd i firmy, które – również fizycznie – w większości znajdują się na terytorium Ameryki. Kraje, które od zawsze obawiają się skutków takiej przewagi, takie jak Chiny i Rosja, zainwestowały w alternatywne rozwiązania, na przykład Wielki Firewall Chiński, państwowe cenzurowane systemy wyszukiwania oraz znacjonalizowane konstelacje satelitów zapewniające usługi nawigacyjne na podobieństwo GPS-u. Ameryka pozostaje jednak hegemonem i sprawuje pieczę nad głównymi wyłącznikami, którymi może odciąć od sieci prawie każdego, kiedy tylko zechce.

Gdy opisuję internet jako z gruntu amerykański, mam na myśli nie tylko infrastrukturę, ale również oprogramowanie (Microsoft, Google, Oracle) i sprzęt (HP, Apple, Dell). Wszystko, od procesorów i innych układów scalonych (Intel, Qualcomm) przez routery i modemy (Cisco, Juniper) po

usługi i platformy internetowe zapewniające dostęp do poczty elektronicznej, sieci społecznościowych i przechowywania danych w chmurze (Google, Facebook i najważniejszy pod względem strukturalnym, choć zupełnie „niewidzialny” Amazon, którego chmurowe usługi wykorzystują rząd Stanów Zjednoczonych i połowa internetu). Niektóre z tych firm produkują urządzenia w innych krajach, na przykład w Chinach, ale są zarejestrowane w Ameryce i obowiązuje je amerykańskie prawo. Rzecz w tym, że w związku z powyższym muszą przestrzegać również tajnych amerykańskich rozporządzeń, wypaczających regulacje prawne i pozwalających rządowi amerykańskiemu szpiegować praktycznie każdego mężczyznę, kobietę i dziecko, którzy kiedykolwiek mieli kontakt z komputerem lub skorzystali z telefonu.

Jeśli zważyć na zamerykanizowany charakter światowej infrastruktury łącznościowej, staje się oczywiste, że rząd Stanów Zjednoczonych posunie się do masowej inwigilacji. A już na pewno powinno to być oczywiste dla mnie. Tymczasem nie było. Chyba głównie dlatego, że rząd konsekwentnie zaprzeczał, jakoby dopuszczał się takiego postępowania; odżegnywał się od tego rodzaju praktyk w sądach oraz mediach z taką stanowczością, że niedowiarkowie oskarżający administrację o kłamstwa, a uchowała się ich ledwie garstka, sprawiali wrażenie szalonych wyznawców teorii spiskowych. Ich podejrzenia dotyczące tajnych programów szpiegowskich NSA wydawały się równie odrealnione, co urojenia paranoików przeświadczonych, że odbiorniki ukryte w naszych zębach rejestrują sygnały wysyłane przez obcych. Wszyscy – ja, ty, my ogółem – byliśmy zbyt ufni. Dla mnie jednak odkrycie prawdy o działaniu służb wywiadowczych stało się szczególnie przykre, ponieważ nie był to pierwszy raz, kiedy dałem się oszukać. Wcześniej poparłem inwazję na Irak i wstąpiłem do wojska. Od chwili, gdy zacząłem pracę dla wywiadu, żyłem

w przekonaniu, że taka sytuacja się nie powtórzy. Miałem przecież poświadczenie bezpieczeństwa kategorii „ściśle tajne”, które, jak sądziłem, gwarantowało mi pewien poziom transparentności. Rząd nie miał przecież powodu, by ukrywać cokolwiek przed osobami odpowiedzialnymi za ukrywanie jego tajemnic. Chcę przez to wszystko powiedzieć, że pewne oczywistości były dla mnie kiedyś nie do pomyślenia. Zmieniło się to dopiero pewien czas po przeprowadzce do Japonii, dokąd przeniosłem się w 2009 roku, by podjąć tam pracę dla NSA, największej amerykańskiej agencji zajmującej się rozpoznaniem elektromagnetycznym.

Była to moja praca marzeń nie tylko dlatego, że wiązała mnie z najbardziej zaawansowaną technologicznie agencją wywiadowczą świata, ale również ze względu na Japonię – kraj, który od małego fascynował Lindsay i mnie. W Japonii czujesz się tak, jakbyś przeniósł się w przyszłość. Oficjalnie miałem być pracownikiem kontraktowym, ale wymiar obowiązków i przede wszystkim lokalizacja wystarczyły, żeby mnie zachęcić. Jest szczypta ironii w tym, że tylko dlatego, iż po raz kolejny zatrudniła mnie prywatna firma, zrozumiałem, co robi mój rząd.

Na papierze pracowałem w Perot Systems, firmie powołanej do życia przez nadpobudliwego Teksańczyka o niepozornej posturze, a przy tym założyciela Partii Reform i dwukrotnego kandydata w wyborach na prezydenta Stanów Zjednoczonych. Kilka dni po moim przybyciu do Japonii firma Perot Systems została sprzedana Dellowi, co spowodowało, że oficjalnie stałem się pracownikiem tego drugiego przedsiębiorstwa. Podobnie jak w CIA status pracownika kontraktowego był czystą formalnością i formą przykrywki. Od pierwszego do ostatniego dnia pracowałem w placówce NSA.

Należący do NSA Pacific Technical Center (PTC, Pacyficzny Ośrodek Techniczny) zajmował połowę budynku na terenie gigantycznej Bazy

Powietrznej Yokota. Jak przystało na siedzibę główną dowództwa amerykańskich sił zbrojnych w Japonii, bazę otaczały wysokie mury ze stalowymi bramami i posterunki obsadzone przez uzbrojonych żołnierzy. Kompleks znajdował się w odległości krótkiej przejażdżki rowerem od Fussa – miasta na zachodnim obrzeżu potężnej metropolii tokijskiej – gdzie mieszkaliśmy z Lindsay.

PTC obsługiwał całą pacyficzną infrastrukturę NSA i zapewniał wsparcie placówkom agencji w okolicznych krajach. Działalność większości tych jednostek koncentrowała się na korzystaniu z tajnych porozumień, które pozwalały NSA instalować urządzenia szpiegowskie w krajach leżących nad Oceanem Spokojnym. W zamian za to NSA obiecywała tamtejszym rządom, że podzieli się z nimi zdobytymi informacjami wywiadowczymi – pod warunkiem, że obywatele rzeczonych państw nie dowiedzą się niczego na temat tej działalności. Najważniejszym celem misji PTC było przechwytywanie sygnałów łącznościowych. Ośrodek gromadził „wycinki” zdobytych przekazów i słał je na drugą stronę oceanu, na Hawaje, skąd z kolei wędrowały do kontynentalnych Stanów Zjednoczonych.

Oficjalnie pełniłem rolę analityka; do moich obowiązków należało utrzymywanie lokalnych systemów NSA, ale w większości zadania, które otrzymywałem na początku, należały raczej do kompetencji administratora systemów i polegały na łączeniu architektury systemowej NSA z tą wykorzystywaną przez CIA. Podróżowałem też do ambasad Stanów Zjednoczonych, podobnych do tej w Genewie, gdzie zakładałem łącza umożliwiające agencjom wymianę informacji wywiadowczych metodami, które wcześniej nie były możliwe, i dbałem o ich poprawne funkcjonowanie. Pierwszy raz w życiu zdałem sobie wówczas sprawę z władzy, jaką posiada osoba rozumiejąca nie tylko wewnętrzną logikę

jednego systemu, lecz również sposób, w jaki współpracuje on – bądź nie daje się pogodzić – z wieloma innymi. Kiedy dyrekcja PTC dostrzegła, że mam talent do niestandardowego rozwiązywania ich problemów, poluzowała mi trochę smycz i pozwoliła przedstawiać własne pomysły.

Dwie cechy NSA zaszokowały mnie już na samym początku. Pierwsza – jak niesamowicie zaawansowana była to agencja w porównaniu z CIA, i druga – jak nonszalancko podchodziła do kwestii bezpieczeństwa na każdym możliwym poziomie, od zarządzania dostępem do informacji po szyfrowanie danych. W Genewie każdego wieczora przed zakończeniem pracy musieliśmy wyjmować z komputerów dyski twarde i zamykać je w sejfie. Co więcej, wszystkie dyski były zaszyfrowane. NSA z kolei nie szyfrowała prawie niczego.

Było coś zdecydowanie niepokojącego w odkryciu, że NSA wysunęła się na prowadzenie w dziedzinie cyberwywiadu, ale pozostawała na szarym końcu w kwestii cyberbezpieczeństwa. Nie dbała nawet o rzecz najbardziej podstawową, czyli zabezpieczenie na wypadek katastrofy. O kopie zapasowe. Każda placówka NSA gromadziła informacje wywiadowcze we własnym zakresie, przechowywała je na własnych lokalnych serwerach i często – ze względu na limity transferu, czyli ograniczenia ilości danych, które można było przesyłać z dużą prędkością – nie wgrywała kopii na główny serwer w siedzibie macierzystej NSA. Skutkiem tego, gdyby jakiekolwiek lokalnie zapisane dane uległy zniszczeniu, ciężka praca włożona w ich zdobycie poszłaby na marne.

Moi szefowie w PTC zdawali sobie sprawę, jak ryzykowne było niesporządzanie kopii wielu agencyjnych plików, zlecili mi zatem, bym opracował rozwiązanie tego problemu i przedstawił je decydentom z siedziby głównej. Poskutkowało to uruchomieniem systemu tworzenia kopii zapasowych i magazynowania danych, pełniącego funkcję cienia

NSA: pełnej, zautomatyzowanej, nieustannie aktualizowanej kopii wszystkich najważniejszych materiałów agencji, która miała umożliwić ponowne uruchomienie wszystkich procesów i zachowanie archiwów w nienaruszonym stanie, nawet gdyby z Fortu Meade zostały dymiące zgliszcza.

Największa trudność związana z tworzeniem globalnego systemu pokryzysowego odzyskiwania danych – a w rzeczywistości dowolnego systemu kopii zapasowych plików z oszałamiającej liczby komputerów – wynika z konieczności obsługi zduplikowanych informacji. Mówiąc prościej: musisz radzić sobie z sytuacjami, kiedy, dajmy na to, tysiąc komputerów ma na dysku identyczny plik. Twoim zadaniem jest zadbać, by nie wysyłały go tysiąc razy, ponieważ wymagałoby to tysiąc razy większych przepustowości i pojemności nośnika. To przede wszystkim właśnie marnotrawna duplikacja uniemożliwiała placówkom agencji codzienne przesyłanie kopii zapasowych do Fortu Meade. Oznaczałoby to zapychanie połączenia tysiącami replik tego samego pliku zawierającego tę samą przechwyconą rozmowę telefoniczną, podczas gdy agencji potrzebna była tylko jedna.

Problemu tego można uniknąć poprzez tak zwaną deduplikację, czyli metodę pozwalającą ocenić unikatowość danych. System, który zaprojektowałem, nieustannie skanował pliki we wszystkich ośrodkach, gdzie NSA przechowywała informacje, i bardzo szczegółowo testował każdy blok danych, by określić jego unikatowość. Pozwoliło to przeistoczyć rzekę danych przepływających wcześniej przez transpacyficzne łącze światłowodowe agencji w wąską strużkę. Algorytm umieszczał w kolejce plików do przesłania wyłącznie te, których kopii NSA nie posiadała w siedzibie głównej.

Połączenie deduplikacji i ciągłego rozwoju technologii magazynowania danych umożliwiło agencji przechowywanie informacji wywiadowczych przez coraz dłuższy czas. Kiedy zaczynałem pracę, osiągnięciem było zachowanie danych na kilka dni. Na przestrzeni mojej kilkuletniej kariery dni zmieniły się w tygodnie, potem w miesiące, a następnie w okres pięciu lat od pozyskania albo jeszcze dłuższy. Możliwe, że w momencie wydania tej książki NSA będzie w stanie przechowywać pliki przez dziesiątki lat. Agencja zwykle zakładała, że nie ma sensu gromadzić informacji, których nie da się przechować do chwili, kiedy staną się użyteczne. Tego zaś nie sposób było przewidzieć. Logika ta leżała u podstaw największego marzenia agencji, a była nim permanencja – zbudowanie systemu umożliwiającego przechowywanie wszystkich zgromadzonych plików w nieskończoność i stworzenie pamięci idealnej. Nieulotnej.

Pracowników NSA obowiązuje złożony protokół określający zasady nadawania nazw kodowych swoim programom. Ma on postać procedury stochastycznej, która jako żywo przypomina wróżenie z chińskiej *Księgi przemian* i polega na losowym doborze wyrazów z dwóch pul. Strona dostępna poprzez wewnątrzagencyjną sieć rzuca wirtualne kości i wybiera jedno słowo z kolumny A oraz drugie z kolumny B, co skutkuje rozmaitymi pozbawionymi znaczenia nazwami w rodzaju FOXACID albo EGOTISTICALGIRAFFE. Stosowanie nazwy kodowej ma sens tylko wówczas, gdy nie odnosi się w żaden sposób do celów danego programu. (Z reportaży prasowych wiemy, że FOXACID był nazwą kodową serwerów, na których NSA przechowywała złośliwe wersje popularnych witryn, zaś EGOTISTICALGIRAFFE to program NSA wykorzystujący specyficzną podatność na atak niektórych przeglądarek internetowych podczas korzystania z sieci Tor; sam Tor pozostawał dla NSA nie do ruszenia). Agenci NSA byli jednak tak pewni swojej pozycji i absolutnej

nietykalności agencji, że rzadko przestrzegali przepisów. Innymi słowy: oszukiwali i powtarzali rzut kośćmi, aż wylosowali kombinację wyrazów, która była ich zdaniem wystarczająco odlotowa, na przykład TRAFFICTHIEF, jak nazwali system do przygotowywania ataków na sieci VPN.

Przyrzekam, że nie postępowałem w ten sposób, gdy chciałem nadać kryptonim swojemu systemowi sporządzania kopii zapasowych. Słowo honoru, że wylosowałem nazwę kodową EPICSHELTER za pierwszym razem.

W późniejszym okresie, kiedy NSA wdrożyła mój system, przemianowała go na Plan (lub Program) Modernizacji Magazynu Danych. Na przestrzeni dwóch lat od chwili, gdy zaprojektowałem EPICSHELTER, system w zmodyfikowanej formie trafił do powszechnego użytku pod kolejną nazwą.

Materiały, które przekazałem dziennikarzom w 2013 roku, dokumentowały tak szeroki wachlarz nadużyć NSA dokonywanych za pomocą tak różnorodnych środków technologicznych, że żaden agent, nawet administrator systemu informatycznego, nie miał szans dowiedzieć się o nich wszystkich, wykonując po prostu codzienne obowiązki. Aby odkryć choćby ułamek nieprawidłowości, trzeba było szukać. A zanim zacznie się czegoś szukać, trzeba wiedzieć, że to coś istnieje.

Źródłem moich pierwszych podejrzeń, do czego dążyła NSA, była sprawa banalna, a mianowicie pewna konferencja.

Kiedy pracowałem nad systemem EPICSHELTER, moja placówka NSA zorganizowała finansowaną przez Międzyagencyjną Akademię Szkolenia Kontrwywiadowczego (JCITA, Joint Counterintelligence Training Academy) konferencję na temat Chin z myślą o Agencji Wywiadu

Departamentu Obrony (DIA, Defense Intelligence Agency), która specjalizowała się w inwigilacji sił zbrojnych oraz szpiegowaniu wszystkiego, co wiąże się z aspektami militarnymi obcych krajów. Na konferencji specjaliści ze wszystkich służb wywiadowczych – NSA, CIA, FBI i wywiadu wojskowego – wygłaszali referaty na temat metod, za których pomocą chiński wywiad atakował amerykański, i co ten ostatni mógł zrobić, żeby utrudnić życie chińskim szpiegom. Choć Chiny leżały w kręgu moich zainteresowań, moja praca nie dotyczyła zagadnień poruszanych na konferencji. Nie poświęcałem zatem wystąpieniom większej uwagi aż do chwili, kiedy dotarło do mnie ogłoszenie, że jedyny informatyk wśród prelegentów musiał w ostatniej chwili odwołać swój udział. Nie jestem pewien, co spowodowało jego nieobecność – może grypa, a może kismet – ale dyrektor kursu, w którym miał brać udział, zapytał, czy w ośrodku pracuje ktoś, kto mógłby zastąpić prelegenta, ponieważ było za późno, by przełożyć wykład. Jeden z kierowników ośrodka wspomniał o mnie, a kiedy spytano mnie, czy chcę spróbować, odpowiedziałem, że tak. Lubiłem mojego szefa i chciałem mu pomóc. Poza tym obudziła się moja ciekawość i cieszyła mnie okazja, by wyjątkowo zająć się czymś, co nie dotyczyło deduplikacji danych.

Szef był wniebowzięty. Po chwili wyjawił jednak, na czym polega haczyk: szkolenie miało odbyć się następnego dnia.

Zadzwoniłem do Lindsay i powiedziałem, że nie wrócę do domu. Zamierzałem poświęcić całą noc na przygotowanie się do prezentacji, której oficjalnym tematem było przenikanie się bardzo starej dyscypliny – kontrwywiadu – z zupełnie nową – cyberwywiadem – w celu udaremniania wrogich działań wywiadowczych w internecie i obrócenia ich na własną korzyść. Zacząłem ściągać z sieci NSA (i CIA, bo do niej wciąż miałem dostęp) wszystkie ściśle tajne raporty na temat chińskiej działalności

internetowej, które udało mi się znaleźć. Skupiłem się na *intrusion sets*, czyli zestawach danych o atakach o zbliżonym typie, wykorzystujących podobne narzędzia i przeprowadzonych do osiągnięcia pokrewnych efektów. Analitycy wywiadu wykorzystują je do identyfikacji grup hakerskich, a także chińskich wojskowych zespołów cyberwywiadowczych, podobnie jak detektywi, którzy w celu rozpoznania sprawcy serii włamań analizują wspólne cechy miejsc przestępstwa albo tryb działania włamywacza.

Postanowiłem zapoznać się z tym mocno rozproszonym materiałem, ponieważ zależało mi, by nie ograniczać się do zaraportowania, w jaki sposób Chińczycy nas hakują. Moim głównym celem było streścić słuchaczom aktualny stan wiedzy sił wywiadowczych o zdolności Chin do elektronicznego śledzenia amerykańskich agentów i źródeł operujących na terenie Państwa Środka.

Wszyscy wiedzą (albo wydaje im się, że wiedzą) o drakońskich ograniczeniach narzucanych na internet przez chiński rząd. Niektórzy też zdają sobie sprawę (albo zdaje im się, że tak jest) z rozmiaru naruszeń wynikających z możliwości rządu mojego kraju, o czym w 2013 roku raportowałem dziennikarzom. Weź jednak pod uwagę, że rzucić stwierdzenie – w stylu antyutopijnej literatury science fiction – iż rząd teoretycznie jest w stanie widzieć i słyszeć wszystko, co robią mieszkańcy danego kraju, to coś zupełnie innego niż rzeczywista próba implementacji takiego systemu. Rozwiązania, które pisarz fantastyki naukowej może zawrzeć w jednym zdaniu, wymagają skoordynowanej pracy tysięcy specjalistów i sprzętu wartego miliony dolarów. Podczas lektury o technicznych szczegółach inwigilacji prywatnej łączności w Chinach – oraz studiowania kompletnego i zgodnego ze stanem rzeczywistym opisu mechanizmów i sprzętu potrzebnych do nieustannego gromadzenia,

przechowywania i analizy miliardów codziennych rozmów telefonicznych i przekazów internetowych generowanych przez ponad miliard osób – doznałem absolutnego szoku. Był to system tak śmiały, będący tak ogromnym osiągnięciem, że w pierwszej chwili prawie zapomniałem zbulwersować się faktem, że stanowi narzędzie totalitarnej kontroli.

Chiny są przecież zdeklarowanym antydemokratycznym państwem jednopartyjnym. Agenci NSA w nawet większym stopniu niż większość Amerykanów byli przeświadczeni, że Państwo Środka jest jednym wielkim autorytarnym piekłem. Niezależnie od tego, jak było w rzeczywistości, wolności obywatelskie mieszkańców Chin nie wchodziły w zakres moich obowiązków. Nie mogłem w tej kwestii nic poradzić. Byłem przekonany, że pracuję dla tych dobrych, więc sam z pewnością jestem dobry.

Zaniepokoiły mnie jednak niektóre aspekty czytanych przeze mnie materiałów. Przypomniałem sobie o pewnej zasadzie, chyba jednej z tych fundamentalnych, która dotyczy rozwoju technologicznego: jeśli coś da się zrobić, to najprawdopodobniej ktoś to zrobi albo już zrobił. Po prostu nie było sposobu, by Ameryka – posiadająca tak wiele informacji na temat poczynań Chińczyków – nie uciekła się do dokładnie takich samych metod. Do mojej podświadomości wdarło się poczucie, że choć poznawałem sytuację poprzez materiały na temat Chin, spoglądałem w lustro, w którym odbijała się Ameryka. Istniała możliwość, że tak samo jak Chiny jawnie traktowały swoich obywateli, Ameryka mogła traktować cały świat… i prawdopodobnie tak właśnie było.

Możesz mnie za to znienawidzić, ale muszę przyznać, że wtedy stłamsiłem niepokój, który we mnie narastał. Zrobiłem wszystko, by go zignorować. W mojej głowie wciąż istniały wyraźne różnice pomiędzy stronami. Wielki Firewall Chiński był formą wewnątrzpaństwowej represji i cenzury – zaprojektowano go z myślą o tym, by w jak najbardziej

demonstracyjny, zniechęcający potencjalnych rebeliantów sposób trzymać obywateli Chin w obrębie muru, a Amerykę na zewnątrz. Tymczasem amerykańskie systemy były niewidoczne i pełniły funkcję czysto obronną. Rozumiałem cyberwywiad Stanów Zjednoczonych tak, że osoby z całego świata mogły korzystać z amerykańskiej infrastruktury i sięgać po dowolną treść, filtrowaną i blokowaną tylko w takim zakresie, jaki uznały za słuszne ich własne kraje i amerykańskie korporacje, a te – w założeniu – nie podlegają kontroli rządu USA. Śledzony i szczegółowo analizowany był w moim mniemaniu wyłącznie ruch internetowy tych, którzy stali się celami ze względu na odwiedzanie na przykład stron o atakach bombowych przeprowadzonych przez dżihadystów albo targowisk złośliwego oprogramowania.

Tak pojmowany model amerykańskiego wywiadu nie budził u mnie żadnych wątpliwości. Wręcz odwrotnie – w pełni popierałem obronną, precyzyjnie nakierowaną inwigilację i stosowanie firewalla – wirtualnej ściany ognia, przez którą mógł przejść każdy uczciwy, podczas gdy jej płomienie dosięgały tylko tych winnych.

Rzecz w tym, że podczas bezsennych dni, które nastąpiły po tamtej bezsennej nocy, w moim umyśle wciąż tliły się podejrzenia. Jeszcze długo po tym, jak przeprowadziłem szkolenie na temat Chin, nie mogłem przestać drążyć tematu.

Kiedy rozpocząłem pracę dla NSA w 2009 roku, miałem tylko odrobinę większe pojęcie o działalności tej agencji niż reszta świata. Z reportaży prasowych wiedziałem, że NSA realizowała dziesiątki programów wywiadowczych autoryzowanych przez prezydenta George’a W. Busha w następstwie ataków na World Trade Center. Przede wszystkim jednak zdawałem sobie sprawę z inicjatywy, która spotkała się z najsilniejszym

publicznym sprzeciwem – chodzi o podsłuch bez nakazu sądowego, stanowiący jeden z punktów Prezydenckiego Programu Inwigilacji (President's Surveillance Program, PSP). Dzięki odwadze kilku demaskatorów z NSA i Departamentu Sprawiedliwości jego istnienie ujawnił w 2005 roku „New York Times".

Oficjalnie PSP należał do dekretów prezydenckich – zasadniczo stanowił zestaw poleceń, który rząd Stanów Zjednoczonych musiał traktować na równi z publicznie ustanawianym prawem, nawet jeśli prezydent nagryzmolił je w tajemnicy na serwetce. PSP dawał NSA prawo zapisywania rozmów telefonicznych i komunikatów internetowych przepływających pomiędzy Stanami Zjednoczonymi a innymi krajami. Co najważniejsze, PSP umożliwiał NSA działanie bez pozyskania specjalnego nakazu od Sądu do spraw Wywiadu Zagranicznego. Jest to tajny trybunał, a jego zadanie polega na wydawaniu upoważnień do stosowania technik inwigilacyjnych; został założony w 1978 roku, kiedy odkryto, że służby wywiadowcze szpiegowały obywateli amerykańskich zaangażowanych w protesty przeciwko wojnie w Wietnamie i w obronę praw obywatelskich.

Po skandalu, który rozpętał się po reportażach w „New York Timesie", oraz próbach podważenia zgodności programu z konstytucją, które podjęli działacze na rzecz wolności obywatelskich z American Civil Liberties Union w zwykłych, jawnych sądach, rząd George'a W. Busha wydał oświadczenie, że Prezydencki Program Inwigilacji wygasa w 2007 roku. To jednak okazało się farsą. Podczas ostatnich dwóch lat urzędowania Busha juniora w Białym Domu Kongres zatwierdził ustawy, które wstecznie legalizowały działania NSA i objęły immunitetem operatorów telekomunikacyjnych oraz dostawców internetu biorących udział w programie. Ustawy te – Protect America Act z 2007 roku i FISA Amendments Act z 2008 roku – posługiwały się umyślnie mylącym

językiem mającym zapewnić obywateli Stanów Zjednoczonych, że ich łączność nie jest bezpośrednio monitorowana, tymczasem w rzeczywistości zwiększały uprawnienia NSA ponad te zapewnione agencji przez program PSP. Wcześniej NSA mogła gromadzić wyłącznie przekazy przychodzące z innych krajów, tymczasem nowa ustawa dawała jej prawo do nasłuchiwania bez nakazu sądowego rozmów telefonicznych i komunikatów internetowych, które wędrowały z terenu USA zagranicę.

Powyższy obraz sytuacji nakreśliłem po przeczytaniu oficjalnego rządowego podsumowania udostępnionego opinii publicznej w lipcu 2009 roku – zresztą to samo lato poświęciłem na rozgryzanie chińskiej zdolności cyberwywiadowczej. Raport ten, sporządzony przez biura inspektora generalnego pięciu organizacji (Departamentu Obrony, Departamentu Sprawiedliwości, CIA, NSA i Biura Sekretarza Krajowego Wywiadu) i opublikowany pod niewiele mówiącym tytułem *Unclassified Report on the President's Surveillance Program* (Jawny Raport o Prezydenckim Programie Inwigilacji), miał zastąpić pełnoprawne dochodzenie Kongresu w sprawie nadużyć NSA za rządów Busha. Fakt, iż prezydent Obama po dojściu do władzy nie domagał się od Kongresu pełnego zbadania sytuacji, był – przynajmniej dla mnie – pierwszą oznaką, że nowy gospodarz Białego Domu (Lindsay entuzjastycznie udzielała się w jego kampanii) nie zamierzał odpowiednio rozliczyć się z przeszłością. W miarę jak jego rząd nadawał różnym programom związanym z PSP nowe nazwy i odnawiał stosowne upoważnienia, nadzieja, którą wspólnie z Lindsay pokładaliśmy w Obamie, okazywała się coraz bardziej płonna.

Upubliczniony raport zawierał głównie informacje, które już znałem, ale pod pewnymi względami okazał się pouczający. Pamiętam, że natychmiast zwrócił moją uwagę dziwaczny ton wywołujący wrażenie, że autorzy mają coś do ukrycia, oraz co najmniej kilka miejsc, gdzie logika

i język pozostawiały wiele do życzenia. Raport bronił legalności różnych programów wywiadowczych, choć rzadko wymieniał je z nazwy i jeszcze rzadziej opisywał. Nie umknęło również mojej uwadze, że prawie żaden z przedstawicieli władzy wykonawczej osobiście zatwierdzający te programy nie zgodził się na przesłuchanie przez inspektorów generalnych. Począwszy od wiceprezydenta, Dicka Cheneya, i prokuratora generalnego, Johna Ashcrofta, po prawników z Departamentu Sprawiedliwości, Davida Addingtona i Johna Yoo, prawie wszyscy liczący się gracze odmówili współpracy ze strukturami, których zadaniem było rozliczać służby wywiadowcze ze skutków ich działań. Z racji tego zaś, że nie było to formalne dochodzenie zobowiązujące do składania zeznań, inspektorowie generalni nie mogli zmusić tych osób do współpracy. Trudno mi było uznać nieobecność decydentów w oficjalnej wersji wydarzeń za cokolwiek innego niż przyznanie się do bezprawnych działań.

Kolejną zaskakującą cechą raportu były powtarzające się tajemnicze odniesienia do zapisywanych wielkimi literami „Innych Działań Wywiadowczych”. Wyczytałem, że nie było dla nich „akceptowalnego uzasadnienia prawnego” ani „podstawy prawnej” poza twierdzeniem prezydenta Busha o nadzwyczajnej władzy wykonawczej przysługującej prezydentowi podczas wojny – tej samej, której końca nie było widać. Rzeczone odniesienia nie opisywały oczywiście w najmniejszym nawet stopniu, o jakie działania może chodzić. Proces dedukcji wskazywał jednak na prawo do inwigilacji celów na terenie Stanów Zjednoczonych bez uzyskania nakazu sądowego, ponieważ była to zasadniczo jedyna czynność wywiadowcza, której nie uprawomocniała żadna ze struktur prawnych utworzonych w następstwie Prezydenckiego Programu Inwigilacji.

Czytając dalej, zacząłem mieć wątpliwości, czy jakikolwiek przytaczany w raporcie fakt w pełni uzasadniał machinacje prawne. Nie

rozumiałem, co wywołało groźby rezygnacji ówczesnego zastępcy prokuratora generalnego, Jamesa Comeya, i dyrektora FBI, Roberta Muellera, jeśli rząd na nowo autoryzuje pewne elementy PSP. Nie znalazłem też niczego, co w pełni wyjaśniałoby, dlaczego tak wielu pracowników NSA – agentów o randze znacznie wyższej niż moja, posiadających dziesiątki lat doświadczenia – i członków personelu Departamentu Sprawiedliwości podjęło ryzyko nawiązania kontaktu z prasą i wyrażenia sprzeciwu wobec tego, jak nadużywane były pewne aspekty PSP. Skoro wszystkie te osoby kładły na szali swoje kariery, rodziny, a nawet życie, sprawa nie mogła kończyć się na podsłuchach bez nakazu, który to temat przewinął się już wcześniej przez pierwsze strony gazet.

Podejrzenia te spowodowały, że ruszyłem na poszukiwania poufnej wersji raportu. Odkrycie, że najwyraźniej nie istniał, ani trochę nie poprawiło mojego samopoczucia. Nie rozumiałem tego. Skoro utajona wersja była po prostu listą grzechów przeszłości, powinienem bez problemu zdobyć do niej dostęp. Nie mogłem jednak nigdzie jej znaleźć. Zacząłem się zastanawiać, czy nie szukam w złych miejscach. Po tym, jak poświęciłem sporo czasu na stosunkowo szeroko zakrojone poszukiwania, które nie przyniosły rezultatu, postanowiłem odpuścić. Pozwoliłem życiu biec własnym rytmem, zwłaszcza że miałem pracę do wykonania. Kiedy pytają cię, jak uchronić agentów wywiadu i ich źródła przed wykryciem i egzekucją z polecenia chińskiego ministerstwa bezpieczeństwa narodowego, trudno sobie przypomnieć, co googlowało się tydzień wcześniej.

Dopiero po dłuższym czasie, kiedy już dawno zapomniałem o niemożliwym do odnalezienia raporcie inspektorów generalnych, tajna wersja dosłownie przesmyknęła się przez moje biurko – zupełnie jakby życie chciało udowodnić mi prawdziwość starego powiedzenia, że

najlepszym sposobem, by coś znaleźć, jest przestać szukać. Kiedy pojawił się ów raport, zrozumiałem, dlaczego moje poszukiwania spełzły na niczym: nie mieli do niego wglądu nawet dyrektorzy agencji. Należał do jednej z kategorii ECI (Exceptionally Controlled Information, Szczególnie Kontrolowanych Informacji) obejmującej dokumenty o nadzwyczaj ograniczonym dostępie – niebywale rzadko stosowanej klasy niejawności, po którą rząd sięgał wyłącznie wówczas, gdy chciał mieć pewność, że pewne fakty pozostaną niewidoczne nawet dla osób upoważnionych do wglądu w informacje objęte klauzulą „ściśle tajne". Ze względu na zajmowane stanowisko znałem większość podkategorii ECI wykorzystywanych przez NSA, ale nie tę, do której należał raport. Był on sklasyfikowany następująco: TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN. Oznaczało to mniej więcej tyle, że tylko kilkadziesiąt osób na świecie miało uprawnienia, by go przeczytać.

Ja zdecydowanie do nich nie należałem. Raport trafił do mnie przez pomyłkę: pracownik biura inspektora generalnego NSA zostawił kopię roboczą w systemie, do którego ja, jako sysadmin, miałem dostęp. Nieznana mi dotąd etykieta STLW okazała się „brzydkim słowem": oznaczeniem wskazującym, że dany dokument nie powinien być przechowywany na dyskach o niskim poziomie zabezpieczenia. Dyski te były nieustannie sprawdzane pod kątem tego, czy pojawiają się na nich „brzydkie słowa", a kiedy tylko do tego dochodziło, otrzymywałem powiadomienie. Moim zadaniem w takiej sytuacji było zdecydować, jak najlepiej wyrugować kłopotliwy dokument z systemu. W tym celu musiałem jednak przeanalizować rzecz osobiście, by potwierdzić, że wyszukiwarka „brzydkich słów" nie oflagowała go przez pomyłkę. W większości wypadków wystarczył mi rzut okiem na zawartość. Tym

razem jednak, kiedy tylko otworzyłem plik i zobaczyłem tytuł, wiedziałem, że przeczytam go od początku do końca.

Miałem przed oczami wszystko, czego brakowało w publicznym raporcie. Wszystko, czego nie mogłem dowiedzieć się z przeczytanych reportaży prasowych i czego odmówiono sądom, których poczynania śledziłem. Oto patrzyłem na pełny spis najtajniejszych programów inwigilacyjnych NSA, dyrektyw agencyjnych oraz dekretów Departamentu Sprawiedliwości, za których pomocą podkopano amerykańskie prawo i naruszono postanowienia konstytucji Stanów Zjednoczonych. Po przeczytaniu całości zacząłem rozumieć, dlaczego nikt z pracowników służb wywiadowczych nie przekazał tego raportu dziennikarzom, a żaden sędzia nie mógł zmusić rządu do ujawnienia go w trakcie publicznego procesu. Plik był objęty tak ścisłą klauzulą niejawności, że tożsamość źródła ewentualnego wycieku, chyba że byłby nim sysadmin, zostałaby ustalona prawie natychmiast. Działalność opisana w dokumencie była zaś w tak olbrzymim stopniu nielegalna, że absolutnie żaden rząd nie pozwoliłby opublikować treści w nieocenzurowanej postaci.

Od razu rzuciła mi się w oczy pewna rzecz: raport podany do wiadomości publicznej, który znałem, nie był – jak to zwykle bywa w takich sytuacjach – okrojoną wersją tajnego dokumentu, z której usunięto wrażliwe informacje. Miał zupełnie inną zawartość, a tajna wersja jednoznacznie obnażała fakt, iż treść stanowiła stuprocentowe, starannie spreparowane kłamstwo. Ta dwulicowość wprawiła mnie w osłupienie, szczególnie że właśnie poświęciłem kilka miesięcy na to, by agencja nie gromadziła wielu wersji tych samych plików. Zazwyczaj kiedy ma się do czynienia z dwiema wersjami jednego dokumentu, różnice pomiędzy nimi mają trywialny charakter – tu brakuje przecinka, tam pojawia się

dodatkowe słowo. Tymczasem w wypadku tych dwóch raportów jedynym, co je łączyło, był tytuł.

Podczas gdy jawna wersja informowała wyłącznie o tym, że po ataku na World Trade Center NSA otrzymała nakaz, by nasilić pozyskiwanie informacji wywiadowczych, wersja tajna opisywała w szczegółach charakter i skalę tego zjawiska. Profil działalności agencji uległ fundamentalnej zmianie: przechwytywanie łączności precyzyjnie określonych celów ustąpiło miejsca masowemu gromadzeniu danych, co jest eufemizmem stosowanym przez NSA na powszechną inwigilację. I podczas gdy jawna wersja raportu broniła rozszerzenia zakresu szpiegowania, strasząc opinię publiczną wizją terroru, tajna wersja opisywała zmianę profilu działalności wprost i przedstawiała ją jako logiczną konsekwencję rosnących możliwości technologicznych.

Sekcja tajnego raportu, za którą odpowiadało biuro inspektora generalnego NSA, przedstawiała zjawisko luk informacyjnych, które powstaje wskutek niemożności gromadzenia danych na bieżąco, i kierowała uwagę czytelnika na fakt, iż istniejące prawo dotyczące działań wywiadowczych (przede wszystkim ustawa o wywiadzie zagranicznym, Foreign Intelligence Surveillance Act) pochodziło z roku 1978, kiedy większość łączności realizowały nadajniki radiowe i linie telefoniczne, a nie światłowody i satelity. Zasadniczo NSA argumentowała, że prędkość dzisiejszej telekomunikacji wyprzedzała, a objętość przerastała amerykańskie prawo – żaden sąd, nawet tajny, nie był zdolny wystawiać nakazów dotyczących konkretnych osób w wymaganym tempie – zaś funkcjonowanie w prawdziwie globalnym świecie wymagało posiadania prawdziwie globalnej agencji wywiadowczej. Wszystko wskazywało, podążając za logiką NSA, na konieczność masowego gromadzenia danych przesyłanych przez internet. Nazwa kodowa programu, w którego ramach

gromadzono te dane, została zawarta w etykiecie rozpoznanej przez mój system jako „brzydkie słowo”: STLW, skrót od STELLARWIND. Inicjatywa ta była jedynym poważnym elementem Prezydenckiego Programu Inwigilacji, którego działalność nie została przerwana – więcej: w tajemnicy przybrała na sile – po tym, jak zostało prasa upubliczniła istnienie programu.

Ze wszystkich tajemnic niejawnej wersji raportu STELLARWIND był największą. Stanowił również największy sekret NSA, i to właśnie dlatego nadano dokumentowi tak ścisłą klauzulę tajności. Samo istnienie programu dowodziło, że misja agencji uległa transformacji – nadal zakładała wykorzystanie technologii, jednak już nie do obrony Ameryki, lecz do panowania nad obywatelami poprzez traktowanie prywatnej łączności internetowej jako potencjalnego źródła elektronicznych informacji wywiadowczych.

W raporcie znalazło się mnóstwo takich oszukańczych redefinicji. Chyba najbardziej zasadniczymi i ewidentnie desperackimi aktami spod tego znaku był szereg manipulacji językowych. STELLARWIND zaczął gromadzić dane z chwilą uruchomienia Prezydenckiego Programu Inwigilacji w 2001 roku, ale trzy lata później – kiedy urzędnicy Departamentu Sprawiedliwości przeciwstawili się kontynuacji programu – administracja George’a W. Busha podjęła próbę uprawomocnienia go *ex post facto* poprzez zmianę znaczenia podstawowych słów, takich jak „zdobyć” i „pozyskać”. Zgodnie z tym, co zostało napisane w raporcie, rząd przyjął stanowisko, że NSA wolno było prowadzić ewidencję dowolnej łączności bez nakazu sądowego, ponieważ z perspektywy prawa zdobywała bądź pozyskiwała informacje dopiero z chwilą, gdy wyszukiwała i pobierała je ze swojej bazy danych.

Ta leksykalna sofistyka wyjątkowo mocno podziałała mi na nerwy, ponieważ dobrze wiedziałem, że celem NSA jest przechowywanie jak największej ilości informacji przez jak najdłuższy czas – najlepiej na wieczność. Jeśli rejestr łączności danej osoby miał być uważany za prawomocnie zdobyty dopiero w chwili, gdy zostanie wykorzystany, mógł spędzić wieczność w bazie danych, formalnie „niepozyskany", pod postacią surowych danych gotowych do dowolnej obróbki. Słowa „zdobyć" i „pozyskać" nie miały już zatem oznaczać wprowadzenia danych do bazy, lecz wysłanie zapytania – w dowolnym, niemożliwym do przewidzenia momencie – przez konkretną osobę (albo, co bardziej prawdopodobne, algorytm) i uzyskanie tak zwanego trafienia. Rząd Stanów Zjednoczonych stawiał się w ten sposób w roli ponadczasowego stróża prawa. Zapewniał sobie możliwość, by w dowolnej chwili przeczesać dane dowolnej osoby, której pogrążenie mogło przynieść korzyść, w poszukiwaniu dowodów przestępstwa (a nie ma na świecie nikogo, czyj rejestr łączności nie zawierałby czegoś obciążającego). Każda kolejna administracja – każdy przyszły skorumpowany albo zbuntowany dyrektor NSA – mogła jakby nigdy nic, z taką samą łatwością, z jaką wciska się włącznik światła, zacząć śledzić dowolną osobę posiadającą telefon albo komputer. Dowiedzieć się, kim jest, czym się zajmuje, gdzie przebywa i w czyim towarzystwie, a także w najdrobniejszych detalach poznać jej przeszłość.

Wyrażenie „powszechna inwigilacja" jest moim zdaniem – i sądzę, że zdaniem większości osób – bardziej przejrzyste w odbiorze niż faworyzowany przez rząd zwrot „masowe gromadzenie danych wywiadowczych", bo ten według mnie daje fałszywe pojęcie o działalności NSA. Masowe gromadzenie danych przywodzi na myśl bibliotekę lub urząd, gdzie praca aż wre. W rzeczywistości zaś mamy do czynienia

z bezprecedensowym działaniem mającym na celu uzyskanie pełnego dostępu do wszystkich informacji przesyłanych drogą cyfrową i ich tajne zapisywanie.

Niestety nawet po ujednoliceniu nomenklatury łatwo o błędne pojmowanie pewnych kwestii. Na przykład ludzie nadal przeważnie myślą o powszechnej inwigilacji w kontekście zawartości, czyli słów, których używają, kiedy rozmawiają przez telefon albo piszą e-mail. Kiedy obywatele odkrywają, że rząd w rzeczywistości niezbyt przejmuje się treścią komunikatów, zaczynają niezbyt przejmować się szpiegowaniem. Ulgę, którą odczuwają, w pewnym sensie łatwo zrozumieć, ponieważ mamy instynktowne przekonanie o tym, jakie elementy naszych wiadomości i wypowiedzi są niepowtarzalne i prywatne. Sądzimy, że to dźwięk naszego głosu, niemal tak unikatowy jak odcisk palca, zdradza naszą tożsamość – albo że robi to niepowtarzalna mina na selfie towarzyszącym tekstowi w MMS-ie. Rzeczywistość jest jednak bardziej niefortunna. Treść rzadko ujawnia o nas tyle, ile inne elementy wymienianych wiadomości. Istnieją niepisane, niewypowiadane formy informacji, które naświetlają szerszy kontekst naszego życia i schematy postępowania.

NSA nazywa je metadanymi. Przedrostek „meta”, tradycyjnie tłumaczony jako „ponad” lub „poza”, tu występuje w znaczeniu „o czymś”: metadane zawierają informacje o innych danych – to zbiór tagów i znaczników, dzięki którym dane stają się użyteczne. Najłatwiej zrozumieć, o co chodzi, na przykładzie tak zwanych danych o aktywności – zapisów dokumentujących wszystko, co robisz na swoich urządzeniach, i co te urządzenia robią bez twojego udziału. Jeśli rozważymy rozmowę telefoniczną, w jej wypadku metadane mogą zawierać datę i godzinę wykonania połączenia, czas trwania, numery, z którego i na który

dzwoniono, oraz miejsca, gdzie rozmawiano. Metadane e-maila mogą z kolei dotyczyć informacji na temat rodzaju komputera, na którym sporządzono wiadomość, czasu i miejsca jej powstania, tożsamości autora i nadawcy, czasu i miejsca wysłania i odbioru, oraz tego, czy ktoś poza nadawcą i odbiorcą miał dostęp do wiadomości, a jeśli tak, to gdzie i kiedy. Metadane mogą powiedzieć osobie inwigilującej, pod jakim adresem spałeś dzisiejszej nocy i o której godzinie wstałeś. Ujawniają wszystkie miejsca odwiedzone w ciągu dnia i informują, ile czasu spędziłeś w każdym z nich. Wskazują, z kim się kontaktowałeś i kto z tobą.

Fakt ten niweczy wszelkie rządowe argumenty, jakoby metadane nie zapewniały bezpośredniego wglądu w sedno komunikacji. Jeśli zważyć na oszałamiającą objętość komunikatów przepływających przez cyfrowe łącza na całym świecie, nie ma możliwości, by przysłuchiwać się każdej rozmowie albo czytać każdy e-mail. A nawet gdyby taka możliwość istniała, korzystanie z niej byłoby stratą czasu, której można uniknąć właśnie dzięki metadanym zawężającym pole poszukiwań. To dlatego nie powinno się traktować metadanych jako niegroźnej abstrakcji, lecz jako esencję treści: są niezaprzeczalnie podstawowym poziomem informacji potrzebnym każdemu, kto chciałby cię inwigilować.

Jeszcze jedna sprawa: treść przekazu zwykle definiuje się jako tę jego część, którą tworzysz świadomie. Wiesz, co mówisz podczas rozmowy telefonicznej i co piszesz w e-mailu. Nie masz jednak prawie żadnej kontroli nad wytwarzanymi przez siebie metadanymi, ponieważ są one generowane automatycznie. Podobnie jak gromadzi, magazynuje i analizuje je maszyna, również maszyna je wytwarza, bez twojego udziału czy nawet zgody. Urządzenia nieustannie komunikują się w twoim imieniu, czy tego chcesz, czy nie. Co więcej, w odróżnieniu od ludzi, z którymi porozumiewasz się z własnego wyboru, urządzenia nie wstrzymują się

przed udostępnianiem prywatnych informacji ani nie korzystają z nazw kodowych w celu zachowania dyskrecji. Wysyłają po prostu do najbliższych nadajników sieci komórkowej sygnały, które nigdy nie kłamią.

Jak na ironię, prawo, które zawsze pozostaje o co najmniej jedną generację technologii z tyłu za postępem, zapewnia znacznie większą ochronę zawartości przekazów niż towarzyszącym im metadanym, choć agencje wywiadowcze są dużo bardziej zainteresowane tymi drugimi. Dostęp do rejestrów łączności pozwala wywiadowi zarówno obserwować sytuację z szerszej perspektywy poprzez analizę danych na ogromną skalę, jak i budować sobie węższy obraz celów dzięki przygotowaniu precyzyjnych map, osi czasu i skojarzeniowych profili działalności, na których podstawie próbuje przewidywać czyjeś postępowanie. Podsumowując, metadane mogą wyjawić osobie, która cię szpieguje, praktycznie wszystko na twój temat, z wyjątkiem tego, co dzieje się w twojej głowie.

Po przeczytaniu tajnej wersji raportu na temat Prezydenckiego Programu Inwigilacji przez kilka tygodni, a może nawet miesięcy byłem w szoku. Ogarnęły mnie smutek i przygnębienie. Końcówka pobytu w Japonii upłynęła mi na próbach zaprzeczania różnym myślom i emocjom.

Miałem wrażenie, że niby znajduję się z dala od domu, ale wciąż jestem nadzorowany. Czułem się bardziej dorosły niż kiedykolwiek, ale skazany na świadomość, że zostaliśmy wszyscy sprowadzeni do jakiegoś zdziecinniałego stanu i zmuszeni do spędzenia reszty życia pod okiem wszechwiedzącego rodzica. Z powodu wymówek, którymi usprawiedliwiałem się przed Lindsay z posępnego nastroju, czułem się jak oszust. Odnosiłem wrażenie, że zrobiłem z siebie idiotę, bo mimo rzekomo zaawansowanych umiejętności informatycznych, pomogłem stworzyć jeden z kluczowych elementów tego systemu i nie domyśliłem się jego

przeznaczenia. Czułem się wykorzystany, bo dopiero teraz zacząłem zdawać sobie sprawę, że jako pracownik służb wywiadowczych od początku chroniłem nie swój kraj, lecz jego struktury. Przede wszystkim zaś miałem poczucie, że cała ta sytuacja pogwałciła moją godność, a konieczność przebywania w Japonii tylko wzmagała przepełniające mnie poczucie zdrady.

Wyjaśnię to.

Mówiony japoński, którego nauczyłem się w college'u dzięki mojemu zainteresowaniu mangą i anime, wystarczał mi do prowadzenia prostych rozmów. Zupełnie inaczej wyglądała sprawa z czytaniem. W japońskim każde słowo może być reprezentowane przez unikalny znak albo kombinację znaków. Symbole nazywają się kanji i jest ich kilkadziesiąt tysięcy – to wiele za dużo, bym zdołał je wszystkie zapamiętać. Często udawało mi się odszyfrować kanji, kiedy towarzyszył im skrypt fonetyczny, furigana, jest on jednak przeznaczony głównie dla osób młodszych albo z zagranicy, zatem nie pojawia się na większości tekstów w miejscach publicznych, na przykład na drogowskazach. Skutkowało to tym, że gdy poruszałem się po mieście, stawałem się funkcjonalnym analfabetą. Myliłem kierunki i skręcałem w prawo, kiedy miałem iść w lewo, i na odwrót. Zapędzałem się w nie te ulice, co trzeba, i zamawiałem z menu w restauracjach nie to, co chciałem. Chodzi mi o to, że byłem tam obcy. Często czułem się zagubiony, i to na kilka sposobów. Parokrotnie podczas wyjazdów z Lindsay na jej fotograficzne eskapady nagle zatrzymywałem się pośrodku wioski albo lasu i docierało do mnie, że nie mam najmniejszego pojęcia, co mnie otacza.

Tymczasem o mnie wiadomo było wszystko. Zrozumiałem, że dla rządu jestem absolutnie transparentny. Telefon, który podpowiadał mi, gdzie iść, i służył radą, kiedy skręciłem w złą stronę, który pomagał mi odczytywać

znaki drogowe i informował o godzinach odjazdu autobusów i tramwajów, dbał jednocześnie o to, by pracodawcy znali wszystkie moje poczynania. Nawet kiedy spoczywał w kieszeni moich spodni, przekazywał moim szefom, kiedy i gdzie się znajduję.

Pamiętam, jak udawałem, że się z tego śmieję, gdy pewnego razu zgubiliśmy się podczas wycieczki, a Lindsay – której niczego nie zdradziłem – spontanicznie stwierdziła:

– Słuchaj, może wyślij SMS-a do Fortu Meade, żeby mogli nas znaleźć… – I żartowała dalej, choć dla mnie nie było to śmieszne: – Halo! – udawała, że rozmawia zamiast mnie. – Poradzicie nam, dokąd teraz iść?

W późniejszym okresie mieszkałem na Hawajach niedaleko Pearl Harbor – miejsca pamiętającego atak, który wciągnął Stany Zjednoczone w prawdopodobnie ostatnią uzasadnioną wojnę. W Japonii byłem bliżej Hiroszimy i Nagasaki, gdzie wojna ta dobiegła niechlubnego końca. Od początku chcieliśmy z Lindsay odwiedzić te miasta, ale za każdym razem, kiedy zaplanowaliśmy wyjazd, coś nam wypadało. Podczas jednego z moich pierwszych wolnych dni zdążyliśmy przygotować się do podróży na południe wyspy Honsiu, do Hiroszimy, ale zostałem wezwany do ośrodka, gdzie polecono mi udać się w przeciwnym kierunku – do Bazy Powietrznej Misawa na skutej lodem północy. W dniu kolejnego zaplanowanego wyjazdu Lindsay się rozchorowała, a później ja zaraziłem się od niej. W nocy poprzedzającej dzień, w którym zamierzaliśmy pojechać do Nagasaki, zostaliśmy obudzeni przez nasze pierwsze poważne trzęsienie ziemi. Zeskoczyliśmy z futonu, zbiegliśmy siedem pięter po schodach i spędziliśmy resztę nocy na ulicy w towarzystwie naszych sąsiadów, trzęsąc się z zimna w piżamach.

Ostatecznie nie pojechaliśmy, czego szczerze żałuję. Hiroszima i Nagasaki to święte miejsca. Stoją tam pomniki, upamiętniające dwieście

tysięcy osób spopielonych przez eksplozję i niezliczone ofiary radioaktywnego opadu, przypominające, że technologia nie ma kompasu moralnego.

Często rozmyślam o „narodzinach atomu”. Wyrażenie to z punktu widzenia fizyki może oznaczać moment, kiedy pewna liczba protonów i neutronów zespaja się w jądro atomowe, ale w najpowszechniejszym rozumieniu odnosi się do rozpoczęcia pewnej ery. Tej, w której nauczyliśmy się wykorzystywać pewne izotopy pierwiastków do wydajniejszej produkcji energii, do wspomagania rolnictwa, do uzdatniania wody, do diagnozy i leczenia śmiertelnych chorób… ale również do budowania bomb atomowych.

Technologia nie ma swojego odpowiednika przysięgi Hipokratesa. Ogromną liczbę decyzji akademickich, przemysłowych, wojskowych i rządowych, podjętych co najmniej od czasu rewolucji przemysłowej, motywowała myśl „czy to się uda?”, a nie „czy powinniśmy?”. Na dodatek intencje przyświecające powstaniu takiej czy innej technologii rzadko, o ile w ogóle, ograniczają zakres jej stosowania.

Nie chcę, rzecz jasna, porównywać broni nuklearnej i cyberinwigilacji pod kątem kosztów ludzkich. Te dwie kwestie mają jednak wiele wspólnego, jeśli chodzi o zjawiska rozprzestrzeniania i rozbrajania.

Jedyne państwa, o których wiem, że w przeszłości na pewno uprawiały masową inwigilację, to obaj pozostali główni uczestnicy drugiej wojny światowej – jeden sprzymierzeniec Ameryki i jeden wróg. Zarówno w Trzeciej Rzeszy, jak i w Związku Socjalistycznych Republik Radzieckich pierwsze jawne sygnały, że inwigilacja ma miejsce, przyjęły powierzchownie niewinną formę spisu powszechnego – oficjalnego zliczenia mieszkańców i utworzenia ich rejestru w celach statystycznych. Pierwszy radziecki spis powszechny z 1926 roku miał poboczny cel.

Wyrażał się on poprzez jawne pytanie o narodowość osób oficjalnie będących obywatelami Związku Radzieckiego. Wyniki spisu przekonały rdzennych Rosjan, którzy tworzyli elitę kraju, że stanowią mniejszość w porównaniu ze zsumowanymi masami uważającymi się za członków różnych narodowości środkowoazjatyckich, między innymi uzbeckiej, kazachskiej, tadżyckiej, turkmeńskiej, gruzińskiej i ormiańskiej. Odkrycie to spotęgowało dążenia Stalina do eradykacji tych kultur poprzez wykorzeniającą „reedukację" w duchu marksistowsko-leninowskiej ideologii.

Organizatorzy niemieckiego spisu powszechnego z 1939 roku podjęli zbliżony gatunkowo projekt statystyczny, dodatkowo wykorzystując techniki komputerowe. Celem było zliczyć populację Rzeszy tak, by ułatwić sprawowanie nad nią kontroli, a także oczyścić ją z pewnych elementów – głównie żydowskich i romskich – przed podjęciem morderczych działań na społeczeństwach zamieszkałych poza granicami Niemiec. Na potrzeby przedsięwzięcia nawiązali współpracę z firmą Dehomag, niemiecką spółką zależną amerykańskiego koncernu IBM, który był właścicielem patentu na tabulator kart perforowanych – swego rodzaju komputer analogowy zliczający otwory wycięte w kartach. Każdego obywatela reprezentowała jedna karta, na niej pewne otwory symbolizowały określone składowe jego tożsamości. Kolumna numer 22 odnosiła się do wyznania: otwór w pozycji 1 oznaczał protestanta, w pozycji 2 katolika, a w pozycji 3 – Żyda. Niewiele później informacje zebrane w ramach spisu posłużyły do rozpoznawania członków europejskiej populacji żydowskiej i deportowania ich do obozów zagłady.

Jeden smartfon bieżącej generacji dysponuje większą mocą obliczeniową niż połączone machiny wojenne Trzeciej Rzeszy i Związku Radzieckiego. Jeżeli będziemy o tym pamiętać, zdołamy lepiej ogarnąć

umysłem zarówno kontekst technologicznej dominacji współczesnego wywiadu amerykańskiego, jak i zagrożenia, jakie taka hegemonia stanowi dla demokratycznych rządów. Na przestrzeni mniej więcej stu lat od wspomnianych spisów powszechnych dokonał się ogromny postęp technologiczny. Niestety nie można tego samego powiedzieć o prawie ani sumieniu – siłach, które mogłyby poskromić jego negatywne skutki.

Stany Zjednoczone, oczywiście, również prowadzą spis powszechny. Jest on konstytucyjnie chronioną instytucją, która na poziomie federalnym pozwala zliczyć populację każdego ze stanów w celu ustanowienia wielkości proporcjonalnej delegacji do Izby Reprezentantów. Ma w pewnym stopniu rewizjonistyczny charakter, ponieważ autorytarne systemy władzy, w tym monarchia brytyjska, która sprawowała zwierzchnictwo nad amerykańskimi koloniami, tradycyjnie wykorzystywały spis powszechny do określania wysokości podatków oraz liczby młodych mężczyzn zdatnych do przymusowej służby wojskowej. Geniusz rozwiązania zawartego w konstytucji polegał na przekształceniu narzędzia opresji w narzędzie demokracji. Spis powszechny, którego organizacja oficjalnie stanowi prerogatywę Senatu, miał być wykonywany co dziesięć lat – był to mniej więcej okres potrzebny na przetworzenie danych z większości spisów, poczynając od pierwszego z roku 1790. Dziesięcioletnie opóźnienie udało się zredukować dopiero w 1890 roku, kiedy po raz pierwszy na świecie zastosowano do spisu komputery (prototyp modelu sprzedanego później faszystowskim Niemcom przez IBM). Technologia obliczeniowa pozwoliła skrócić czas obróbki danych o połowę.

Dziś technologia cyfrowa spowodowała nie tylko dalsze uproszczenie tej ludzkiej księgowości – sprawiła mianowicie, że spisy ludności powoli przestają być potrzebne. Masowa inwigilacja to niekończący się spis

powszechny, zdecydowanie bardziej niebezpieczny niż wszelkie kwestionariusze przesyłane, jak we wcześniejszych latach, pocztą. Wszystkie nasze urządzenia, od smartfonów po komputery, są w zasadzie miniaturowymi modułami gromadzącymi dane demograficzne, a my nosimy je w plecakach i kieszeniach; to wykonawcy spisu powszechnego, którzy wszystko zapamiętują i niczego nie wybaczają.

W Japonii doszło do moich osobistych „narodzin atomu”. To tam zdałem sobie sprawę, w jakim kierunku zmierzają nowe technologie, i że moje pokolenie musi zareagować, jeśli ma powstrzymać ich rosnące panowanie nad naszym życiem. Byłoby tragedią, gdybyśmy znaleźli w sobie siłę woli, by się im przeciwstawić dopiero w chwili, gdy opór stanie się daremny. Przyszłe generacje musiałyby przyzwyczaić się do świata, w którym inwigilacja nie jest zjawiskiem okazjonalnym, precyzyjnie nakierowanym, stosowanym w uzasadnionych prawnie okolicznościach, lecz nieustannym i powszechnym: uchem, które wszystko słyszy, okiem, które wszystko widzi, pamięcią, która nie zasypia i wiecznie trwa.

Z chwilą, gdy władze połączyły masowe gromadzenie danych i ich permanentne przechowywanie, zyskały możliwość wybrania dowolnej osoby bądź grupy i wyszukania – tak samo jak i ja szukałem w agencyjnych plikach – dowodów popełnienia takiego przestępstwa, jakie dla rządzących okazywało się wygodne.

17_Dom_na_chmurze|

Po powrocie do Stanów w dalszym ciągu pracowałem dla Della, który w 2011 roku oddelegował mnie do CIA w charakterze pracownika zewnętrznego. Tak oto ponownie trafiłem do agencji, tyle tylko, że tym razem moim nominalnym pracodawcą była firma Dell. Pamiętam, jak pewnego pogodnego wiosennego popołudnia wróciłem do domu po pierwszym dniu pracy na nowym stanowisku i z pewnym rozbawieniem uświadomiłem sobie, że jestem posiadaczem skrzynki na listy. Było to jedno z tych prostopadłościennych pudeł z indywidualnymi przegródkami, jakie często widuje się przy amerykańskich szeregówkach – nic nadzwyczajnego, ale kiedy je zobaczyłem, mimowolnie się uśmiechnąłem. Od lat nie miałem czegoś takiego i po przeprowadzce do nowego domu ani razu nie przyszło mi do głowy, by sprawdzić jej zawartość. Tamtego dnia zapewne również nie zwróciłbym na skrzynkę uwagi, gdyby nie fakt, że była wypełniona po brzegi – listy nie mieściły się już w środku i część z nich wystawała z przegródki. Jak się okazało, otrzymana przeze mnie korespondencja składała się wyłącznie z przesyłek reklamowych, zaadresowanych do „Pana Edwarda J. Snowdena lub aktualnego lokatora". W kopertach znajdowały się ulotki i kupony zniżkowe na zakup artykułów gospodarstwa domowego. Ktoś wiedział, że niedawno wprowadziłem się do nowego domu.

Kiedy przeglądałem wyjęte ze skrzynki koperty, przypomniałem sobie, jak będąc jeszcze dzieckiem, znalazłem w naszej codziennej poczcie list do mojej siostry. Chciałem go otworzyć, ale moja mama sprzeciwiła się temu.

Zapytałem, dlaczego nie wolno mi tego zrobić.

– Bo nie jest zaadresowany do ciebie – powiedziała mama.

Wyjaśniła mi, że otwieranie cudzej korespondencji – nawet jeśli są to tylko życzenia urodzinowe albo jakiś łańcuszek – jest bardzo nietaktowne. A w dodatku jest to przestępstwo.

Chciałem się dowiedzieć, co to za przestępstwo.

– Całkiem poważne, kolego – odparła moja mama. – To przestępstwo federalne.

Przedarłem koperty z reklamami na pół, po czym wyrzuciłem je do śmieci.

Miałem na sobie nowy garnitur od Ralpha Laurena, w kieszeni nowego iPhone’a, a na nosie nowe okulary firmy Burberry. Miałem też nową fryzurę i klucze do nowego domu w Columbii w stanie Maryland – największego domu, w jakim dotąd mieszkałem, a zarazem pierwszego, w którym czułem się naprawdę u siebie. Byłem bogaty, a przynajmniej za takiego uważali mnie moi przyjaciele. Ledwo się poznawałem.

Doszedłem do wniosku, iż najlepiej będzie udawać, że wszystko jest w porządku, i skupić się na zarabianiu pieniędzy i zapewnieniu lepszego życia moim bliskim – ostatecznie, czy nie tak właśnie postępowali wszyscy dookoła?

Ale łatwiej było powiedzieć, niż zrobić. Mam na myśli udawanie. Bo jeśli mowa o pieniądzach, to ich zarabianie przychodziło mi całkiem łatwo. Tak łatwo, że budziło to we mnie poczucie winy.

Wliczając mój pobyt w Genewie, spędziłem za granicą niemal cztery lata z krótkimi i niezbyt częstymi przerwami na wizyty w domu. Po powrocie miałem nieodparte wrażenie, że Ameryka się zmieniła i że nie był to już ten sam kraj, który opuściłem cztery lata temu. Przesadą byłoby stwierdzenie, że czułem się w Stanach jak obcokrajowiec, ale często

zdarzało się, że nie miałem pojęcia, czego dotyczą rozmowy z moim udziałem. Padały w nich tytuły seriali i filmów, których nigdy nie widziałem, albo nawiązania do skandali celebrytów, o których nigdy nie słyszałem i którzy nic mnie nie obchodzili. W takich chwilach nie wiedziałem, co odpowiedzieć, bo po prostu nie miałem nic do powiedzenia.

Sprzeczne myśli piętrzyły mi się w głowie niczym klocki w *Tetrisie*, a ja starałem się jakoś je uporządkować i sprawić, by zniknęły. Ci wszyscy Bogu ducha winni ludzie – myślałem sobie – to bezbronne ofiary, obserwowane przez rząd za pomocą tych samych ekranów, w które ci biedacy wpatrują się z takim zachwytem. Chwilę później ganiłem się w duchu: uspokój się i przestań dramatyzować – ci ludzie są szczęśliwi, nie obchodzi ich, czy są obserwowani; nie ma powodu, żebyś się tym przejmował. Wykonuj swoją pracę, zarabiaj i płać rachunki. Na tym polega dorosłe życie.

Oboje z Lindsay pragnęliśmy normalnego życia. Byliśmy gotowi zrobić kolejny krok w tym kierunku i postanowiliśmy się ustatkować. Na tyłach naszego nowego domu mieliśmy uroczy ogród, gdzie rosła wiśnia przypominająca mi Japonię, a zwłaszcza pewne miejsce nad rzeką Tama w Tokio; Lindsay i ja lubiliśmy spędzać czas, obserwując opadające płatki kwiatów sakury, śmiejąc się i turlając po pachnącym kwietnym dywanie.

Lindsay starała się o uzyskanie certyfikatu instruktorki jogi, a ja przyzwyczajałem się do mojej nowej posady – w dziale sprzedaży.

Jeden z zewnętrznych wykonawców, z którymi pracowałem przy tworzeniu programu EPICSHELTER, przeszedł później do Della i zaczął mnie przekonywać, że tracę czas, pracując za stawkę godzinową. Tłumaczył, że powinienem przenieść się do działu zajmującego się sprzedażą, ponieważ mógłbym tam zarobić prawdziwą fortunę na pomysłach takich jak EPICSHELTER. Gdybym posłuchał jego rady,

znalazłbym się o wiele szczebli wyżej na drabinie korporacyjnej kariery, a on otrzymałby sowitą premię za polecenie mnie na nowe stanowisko. Byłem gotów dać się przekonać, tym bardziej że przejście do sprzedaży pozwoliłoby mi uwolnić się od narastającego poczucia moralnego dyskomfortu, które prędzej czy później wpędziłoby mnie w tarapaty. Oficjalna nazwa mojego nowego stanowiska brzmiała „konsultant do spraw rozwiązań”. W gruncie rzeczy moja praca polegała na rozwiązywaniu problemów wywoływanych przez współpracującego ze mną menadżera do spraw obsługi klientów, którego będę tu nazywał Cliffem.

Cliff miał być twarzą, a ja mózgiem projektów realizowanych dla CIA. Kiedy spotykaliśmy się z pracownikami agencji odpowiedzialnymi za opłaty licencyjne i pozyskiwanie sprzętu technicznego, rolą Cliffa było za wszelką cenę sprzedać im oferowane przez firmę Dell produkty i usługi. W tym celu składał wiele pięknie brzmiących obietnic dotyczących rzeczy, które mielibyśmy zrobić dla agencji – obietnic daleko wykraczających poza możliwości naszej konkurencji (i nasze również). Moim zadaniem było kierowanie pracami specjalistów; starali się oni opracować coś, co przynajmniej w pewnym stopniu spełniałoby kłamliwe obietnice Cliffa i uchroniłoby nas wszystkich przed wylądowaniem w więzieniu po tym, kiedy ktoś, kto w imieniu agencji podpisał dla nas czek, po raz pierwszy naciśnie przycisk „power”.

Zero presji.

Nasz najważniejszy projekt miał pomóc CIA w nadążaniu za najnowszymi osiągnięciami techniki – a przynajmniej byciu na bieżąco z technicznymi standardami NSA – poprzez zapewnienie agencji dostępu do jednego z najciekawszych i zyskujących coraz większą popularność rozwiązań z dziedziny technologii teleinformatycznych, czyli „prywatnej chmury”. Naszym celem było zintegrowanie procesów przetwarzania

i przechowywania danych, przy jednoczesnej dywersyfikacji metod dostępu do tych informacji. Mówiąc wprost, chodziło o to, żeby pracownik agencji przebywający w namiocie na afgańskim pustkowiu mógł wykonywać dokładnie taką samą pracę i to dokładnie w taki sam sposób, co osoba przebywająca w kwaterze głównej CIA. Kierownictwo techniczne CIA, a właściwie kierownictwo wszystkich agencji zrzeszonych we Wspólnocie Wywiadów, nieustannie narzekało na problem „silosów", czyli miliardów rozproszonych po całym świecie baz danych, których nie można było na bieżąco śledzić ani mieć do nich swobodnego dostępu. Kierowany przeze mnie zespół, składający się z najbardziej łebskich fachowców, jacy pracowali w Dellu, miał wymyślić sposób na to, by każdy uprawniony pracownik agencji mógł uzyskać dostęp do całości zasobów danych z dowolnego miejsca na Ziemi.

W fazie koncepcyjnej nasza chmura dorobiła się roboczej nazwy Frankie. Nie miałem z tym nic wspólnego: w pionie technicznym nazywaliśmy ją po prostu Prywatną Chmurą. Nazwę Frankie wymyślił Cliff, który podczas jednej z prezentacji dla przedstawicieli CIA zapewnił, że pokochają naszego małego Frankensteina, „bo to prawdziwy potwór".

Im więcej obietnic składał Cliff, tym więcej miałem roboty. W rezultacie weekendy stanowiły dla Lindsay i dla mnie jedyną okazję, by spotkać się z bliskimi i przyjaciółmi. Musieliśmy również zająć się umeblowaniem i wyposażeniem naszego nowego domu. Kiedy się wprowadziliśmy, na wszystkich trzech kondygnacjach zastaliśmy jedynie gołe ściany; niektórymi elementami wyposażenia obdarowali nas nasi szczodrzy rodzice, natomiast całą resztę musieliśmy kupić sami. Urządzanie własnego domu wydawało się nam bardzo dojrzałym zajęciem, ale to, jak się do tego zabraliśmy, mówił sporo o naszych priorytetach: kupiliśmy naczynia, sztućce, biurko oraz krzesło, ale wciąż sypialiśmy na

rozłożonym na podłodze materacu. Ponieważ nabrałem wstrętu do kart kredytowych pozwalających śledzić każdy nasz krok, płaciliśmy za wszystko gotówką. Kiedy potrzebowaliśmy samochodu, przejrzałem ogłoszenia i kupiłem używaną acurę integrę rocznik 1998; zapłaciłem za nią trzy tysiące dolarów w gotówce. Nie narzekaliśmy na brak pieniędzy, ale ani Lindsay, ani ja nie lubiliśmy ich wydawać – jedynym wyjątkiem były wydatki na sprzęt komputerowy, a także na różne specjalne okazje. Na Walentynki kupiłem Lindsay rewolwer, o którym zawsze marzyła.

Mieszkaliśmy w odległości dwudziestu minut jazdy od ponad dziesięciu dużych centrów handlowych. Jednym z nich było Columbia Mall – ogromny kompleks o powierzchni stu czterdziestu tysięcy metrów kwadratowych, w którym mieściło się około dwustu sklepów, multipleks AMC z czternastoma salami kinowymi, azjatycka restauracja sieci P.F. Chang’s i cukiernia Cheesecake Factory. Kiedy jeździliśmy naszą zdezelowaną integrą po dobrze znanych mi drogach, byłem pod wrażeniem tego, jak bardzo rozwinął się ten region pod moją nieobecność. Po 11 września 2001 roku amerykański rząd zaczął szastać pieniędzmi na prawo i lewo i najwyraźniej całkiem spora ich część trafiła do kieszeni członków tutejszych społeczności. Poczułem się onieśmielony, a nawet nieco przytłoczony, gdy po dłuższym czasie spędzonym za granicą wróciłem do kraju i uświadomiłem sobie na nowo, jak zamożna była ta część Ameryki i jak wiele możliwości oferowała konsumentom, oddając do ich dyspozycji niezliczone galerie handlowe i ekskluzywne salony wystawowe z artykułami wyposażenia wnętrz. Sklepy te kusiły klientów coraz to nowymi wyprzedażami, czy to z okazji Dnia Prezydenta, czy to Święta Pamięci Narodowej, Dnia Niepodległości, Święta Pracy albo Dnia Weterana. Pod gwiaździstymi sztandarami rozpościerały się

okolicznościowe transparenty reklamowe, zachęcające do skorzystania ze świątecznych obniżek, rabatów i upustów.

Któregoś popołudnia wybraliśmy się z Lindsay do sklepu Best Buy po sprzęt gospodarstwa domowego. Wybraliśmy mikrofalówkę, po czym Lindsay uparła się, żebyśmy rzucili okiem na miksery. Kiedy wyciągnęła telefon i zaczęła sprawdzać, który z dziesięciu dostępnych modeli ma najlepsze opinie wśród internautów, postanowiłem wymknąć się do działu komputerowego na drugim końcu sklepu.

Nie dotarłem tam jednak, bo na skraju działu kuchennego zobaczyłem coś, co sprawiło, że stanąłem jak wryty. Na jasno oświetlonym i udekorowanym podeście stała nowiutka lodówka. Mówiąc ściśle, była to „inteligentna lodówka”; jak informowały reklamowe prospekty, posiadała „dostęp do internetu”.

Omal nie padłem z wrażenia.

Po chwili zbliżył się do mnie sprzedawca, który wziął moje osłupienie za przejaw zainteresowania.

– Coś niesamowitego, prawda? – zagadnął, a następnie zademonstrował kilka funkcji urządzenia.

W drzwi wbudowany był ekran, a obok niego znajdował się uchwyt na rysik – można nim było zapisać na ekranie wiadomość. Zamiast pisać, mogłeś też nagrać wiadomość głosową lub wideo. Oprócz ekranu lodówka posiadała moduł Wi-Fi, dzięki czemu można było z niej korzystać tak samo jak ze zwykłego połączonego z siecią komputera: sprawdzać pocztę elektroniczną, przeglądać kalendarz, oglądać filmiki na YouTubie i odtwarzać muzykę z plików MP3. Można było nawet do kogoś dzwonić. Oparłem się pokusie, by wybrać numer komórki Lindsay i oznajmić jej: „Hej, dzwonię z lodówki”.

Specjalne czujniki monitorowały temperaturę wewnątrz komory chłodzącej, a także skanowały kody kreskowe przechowywanych produktów, monitorując ich świeżość i podając informacje na temat ich wartości odżywczej. Lodówka podsuwała nawet użytkownikowi propozycje przepisów kulinarnych. O ile dobrze pamiętam, kosztowała 9000 dolarów.

– Koszty dostawy w cenie – poinformował sprzedawca.

Pamiętam, że przez całą drogę powrotną do domu milczałem zakłopotany. To, co zobaczyłem na stoisku ze sprzętem AGD, nie do końca było tak niesamowitą, księżycową technologią, jak próbowano nam to wmówić. Byłem przekonany, że „inteligentna lodówka” została wyposażona w funkcję dostępu do internetu tylko po to, by przekazywać producentowi informacje na temat zwyczajów konsumenckich użytkowników, a także wszelkie inne dane dotyczące gospodarstw domowych. Producent mógł następnie zarabiać na sprzedaży tych danych innym podmiotom, a my mieliśmy płacić za przywilej bycia inwigilowanymi.

Zacząłem się zastanawiać, czy jest sens irytować się z powodu narastającej inwigilacji i kontroli ze strony rządu, skoro moi przyjaciele, sąsiedzi i inni współobywatele gotowi byli dobrowolnie zgodzić się na szpiegowanie przez podmioty komercyjne i pozwolić na to, by śledzono ich nie tylko podczas przeglądania zasobów sieci, ale nawet w trakcie przeglądania zasobów własnej lodówki. Kolejny krok w kierunku permanentnej inwigilacji o charakterze komercyjnym został zrobiony pięć lat później, kiedy rozpoczęła się domotyczna rewolucja i gdy zaprosiliśmy do naszych domów „wirtualnych asystentów”, takich jak Amazon Echo czy Google Home. Urządzenia te, ustawiane przez dumnych użytkowników na nocnym stoliku w sypialni, rejestrują i przekazują dalej informacje o naszych czynnościach, nawykach i upodobaniach (a także fetyszach

i perwersjach). Wszystkie te informacje są następnie przekładane na reklamowe algorytmy, przynoszące zysk w żywej gotówce. Dane, które generujemy w naszym codziennym życiu – godząc się na inwigilowanie różnych aspektów naszej codziennej egzystencji – pozwalają bogacić się prywatnym firmom i korporacjom, a zarazem przyczyniają się do zubożania naszego prywatnego życia. O ile rządowa inwigilacja uprzedmiotawia obywatela i wydaje go na łaskę i niełaskę władzy, o tyle ta komercyjna sprawia, że konsument staje się towarem sprzedawanym innym firmom, brokerom baz danych albo agencjom reklamowym.

W tamtym czasie każda duża firma z branży zaawansowanych technologii rozwijała cywilne wersje chmury – usługi, nad którą pracowałem dla CIA. (Cztery lata wcześniej Dell próbował nawet opatentować nazwę *cloud computing*, ale wniosek w tej sprawie został odrzucony przez amerykański urząd patentowy). Ze zdumieniem obserwowałem, jak chętnie ludzie godzą się na korzystanie z chmury. Byli tak podekscytowani perspektywą posiadania łatwo dostępnych kopii swoich filmów, muzyki i e-booków, że nie zastanawiali się nad tym, dlaczego tak wyrafinowana technologicznie i tak praktyczna usługa jest im oferowana za darmo lub półdarmo.

Nie potrafię wskazać żadnego innego produktu czy usługi, które od pierwszej chwili spotkały się z tak entuzjastycznym przyjęciem. Hasło „chmura” przekonało decydentów z CIA do skorzystania z oferty Della, tak jak podbiło serca klientów firmy Apple, Amazon czy Google. Wystarczy, że zamknę oczy i bez trudu mogę przywołać z pamięci głos Cliffa przekonujący jakiegoś ważniaka z CIA, że „dzięki chmurze będziecie w stanie przeprowadzać aktualizacje zabezpieczeń we wszystkich swoich komputerach na całym świecie” albo „po uruchomieniu chmury będziecie mogli sprawdzić, kto przeczytał dowolny zapisany w niej dokument”.

Chmura była biała, puszysta oraz idylliczna, unosiła się gdzieś wysoko ponad niespokojnym światem. Zasnute skłębionymi chmurami niebo może zwiastować burzę, ale pojedyncza chmura rzuca kojący cień. Zapewnia ochronę i wytchnienie. Mam wrażenie, że większości ludzi kojarzyła się z rajem.

Dell podobnie jak wszystkie największe firmy oferujące usługi oparte na chmurze – Amazon, Apple i Google – uważał rozkwit technologii chmurowej za początek nowej epoki przetwarzania danych. Ale przynajmniej teoretycznie był to krok wstecz, cofnięcie się do czasów, gdy systemy obliczeniowe polegały na scentralizowanej architekturze typu mainframe; w takich systemach wielu użytkowników korzystało z jednej, centralnej jednostki przetwarzającej dane, której bezpośrednia obsługa była wyłączną domeną wąskiej kadry specjalistów. Odejście od tego „nieosobistego" modelu nastąpiło stosunkowo niedawno, bo zaledwie jedno pokolenie temu, gdy przedsiębiorstwa takie jak Dell skonstruowały i wypuściły na rynek „osobiste" komputery na tyle tanie i proste w obsłudze, by mogły być atrakcyjne dla zwykłych śmiertelników. Era komputerów osobistych dała początek desktopom, laptopom, tabletom i smartfonom, czyli całej gamie urządzeń pozwalających indywidualnym użytkownikom na wykonywanie ogromnej ilości pracy twórczej. Wkrótce jednak trzeba było odpowiedzieć sobie na pytanie: w jaki sposób przechowywać efekty tej pracy?

Taka właśnie była geneza powstania technologii „przetwarzania w chmurze". Odtąd nie miało już większego znaczenia, jakim komputerem osobistym dysponowałeś, ponieważ polegałeś przede wszystkim na komputerach znajdujących się w ogromnych centrach danych wybudowanych w różnych zakątkach świata przez korporacje oferujące usługi chmurowe. W pewnym sensie był to powrót do rozwiązań typu

mainframe: w centrum danych stoją niezliczone rzędy szaf z identycznymi serwerami, połączonymi ze sobą tak, że wszystkie razem tworzą chmurę obliczeniową. Ewentualna utrata pojedynczego serwera, a nawet całego centrum obliczeniowego przestała stanowić problem, ponieważ poszczególne serwery są jedynie cząstkami globalnej chmury.

Z punktu widzenia przeciętnego użytkownika chmura to po prostu mechanizm przechowywania danych. Twoje dane nie są przechowywane i przetwarzane na prywatnym urządzeniu, tylko na wielu różnych serwerach, mogących stanowić własność wielu różnych firm. W rezultacie te dane nie są już tak naprawdę twoje. Rzeczywistą kontrolę nad nimi sprawują prywatne firmy, które mają prawo wykorzystywać je do niemal dowolnych celów.

Zajrzyj do warunków umowy, jaką podpisałeś z dostawcą usług chmurowych – nawiasem mówiąc, teksty tych umów z roku na rok stają się coraz dłuższe i obecnie liczą zwykle ponad sześć tysięcy słów, czyli dwa razy więcej niż przeciętny rozdział tej książki. Decydując się na przechowywanie plików na zewnętrznych serwerach, często zrzekamy się prawa do decydowania o ich losie. To dostawca usługi stanowi o tym, jakie rodzaje danych będzie dla nas przechowywał, i może skasować te, których przechowywać nie zechce. Jeśli nie zrobiliśmy zawczasu ich kopii i nie zapisaliśmy jej na naszym własnym urządzeniu lub nośniku, to skasowane przez dostawcę usługi dane będą dla nas bezpowrotnie utracone. Jeśli jakieś umieszczone przez nas w chmurze dane wzbudzą szczególne zastrzeżenia, na przykład z uwagi na naruszenie warunków świadczenia usługi, to firma zarządzająca chmurą ma prawo skasować nasze konto i odmówić nam dostępu do danych, a zarazem zachować dla siebie kopię, którą może następnie przekazać dowolnym organom państwowym bez naszej wiedzy i zgody. W ostatecznym rozrachunku ochrona prywatności naszych plików

uzależniona jest od tego, w czyim posiadaniu się znajdują. Dane przechowywane w chmurze to najbardziej prywatna, a zarazem najsłabiej chroniona własność.

Era internetu takiego, na jakim się wychowałem i jaki mnie ukształtował, nieubłaganie się kończyła. Wraz z nią dobiegała końca moja młodość. Korzystanie z sieci, które kiedyś było cudowną przygodą, stawało się najeżoną trudnościami męczarnią. Wyrażanie siebie i własnych poglądów online wymagało przedsiębrania tak daleko posuniętych środków ostrożności, że zupełnie zatracało się przy tym poczucie wolności i satysfakcji. Inwencja i kreatywność schodziły na dalszy plan, a kluczowa stawała się kwestia bezpieczeństwa. Każda internetowa transakcja niosła za sobą ryzyko.

Podmioty z sektora prywatnego tymczasem zajęte były wykorzystywaniem naszego rosnącego uzależnienia od technologii internetowej do konsolidacji rynku usług sieciowych. Większość amerykańskich użytkowników internetu przez całe swoje cyfrowe życie korzysta z poczty elektronicznej, mediów społecznościowych oraz platform handlu elektronicznego należących do potężnego triumwiratu: Google, Facebook i Amazon. Wspólnota Wywiadów postanowiła zrobić z tego użytek i uzyskać dostęp do zasobów sieciowych tych firm – zarówno poprzez urzędowe nakazy, utrzymywane w tajemnicy przed opinią publiczną, jak i w wyniku działań niezgodnych z prawem ukrywanych przed firmami, które tymi działaniami objęto. Dane użytkowników, do tej pory przynoszące pokaźne zyski prywatnym firmom, teraz zaczęły być wykradane przez agencje rządowe. Obserwując to, czułem się bezradny jak jeszcze nigdy dotąd.

Poza uczuciem bezsilności ogarniało mnie coraz częściej osobliwe wrażenie bycia pozostawionym samemu sobie, czemu towarzyszyła świadomość, że naruszana jest moja prywatność. Czułem się zagubiony – fragmenty mojego życia porozrzucane były po rozsianych po całym świecie serwerach – a jednocześnie ograniczany czy też poddany ciągłej presji. Codziennie rano po wyjściu z domu szukałem wzrokiem kamer monitoringu, którymi naszpikowano nasze sąsiedztwo, chociaż wcześniej nie zwracałem na nie uwagi. Za każdym razem, gdy w drodze do lub z pracy oczekiwałem na zmianę świateł na zielone, myślałem o czujnikach i obiektywach, które nieustannie miały mnie na oku, niezależnie od tego, czy przejechałem skrzyżowanie na czerwonym, czy zatrzymałem się zgodnie z przepisami. Wiedziałem, że kamery wyposażone w system rozpoznawania tablic rejestracyjnych odnotowywały każdy mój przejazd, nawet jeśli nie przekraczałem prędkości 35 mil na godzinę.

Podstawowe zasady amerykańskiego systemu prawnego mają na celu utrudnić, a nie ułatwić pracę organom porządku publicznego. I wcale nie jest to błąd ustawodawców, lecz kluczowa cecha demokracji. Organy nadzorujące przestrzeganie prawa w Ameryce mają dokładać starań, by obywatele nie wyrządzali sobie wzajemnie szkody ani krzywdy. Zadaniem sądów z kolei jest powstrzymywanie tychże organów przed nadużywaniem władzy, a także zapewnianie obywatelowi możliwości uzyskania zadośćuczynienia w wypadku naruszenia jego praw przez funkcjonariuszy państwowych, którzy jako jedyni mogą zatrzymywać współobywateli, aresztować ich i używać wobec nich siły, w tym także śmiercionośnej broni. Do najważniejszych ograniczeń nałożonych na organy porządku publicznego należą zakaz prowadzenia inwigilacji obywateli na terenie prywatnym będącym ich własnością, a także zakaz przejmowania prywatnych nagrań bez nakazu sądowego. Istnieją również przepisy, które

ograniczają możliwość monitoringu miejsc publicznych, w tym większości ulic i chodników.

Organy nadzorujące przestrzeganie prawa początkowo wykorzystywały kamery monitoringu umieszczone w miejscach publicznych do odstraszania potencjalnych sprawców czynów zabronionych, a także pomagania śledczym w wykrywaniu sprawców przestępstw już popełnionych. W miarę jednak jak cena tych urządzeń robiła się coraz niższa, stały się właściwie wszechobecne i zaczęły pełnić funkcję prewencyjną – organy porządku publicznego wykorzystywały je do śledzenia osób, które nie tylko nie popełniły żadnego przestępstwa, ale nawet nie były o to podejrzewane. A przecież największe niebezpieczeństwo jest dopiero przed nami – wynika ono z coraz lepszych możliwości sztucznej inteligencji (AI, Artificial Intelligence) w rozpoznawaniu wzorców i twarzy. Kamera monitoringu wizyjnego wyposażona w moduł AI nie byłaby już zwykłym urządzeniem służącym do rejestracji obrazu – stałaby się czymś w rodzaju automatycznego policjanta, prawdziwego robocopa, skanującego obszar w poszukiwaniu wszelkich podejrzanych zachowań, mogących świadczyć na przykład o handlu narkotykami (ludzie obejmujący się lub podający sobie ręce) albo o przynależności danej osoby do ulicznego gangu (noszenie odzieży określonej marki lub w specyficznym kolorze). Już w roku 2011 nie ulegało dla mnie wątpliwości, że zmierzamy właśnie w takim kierunku i że odbywa się to bez żadnej publicznej debaty na ten temat.

Rozmaite przykłady potencjalnych nadużyć w wykorzystaniu technologii monitoringu wizyjnego złożyły się w mojej wyobraźni na okropną wizję przyszłości. Logicznie rzecz ujmując, świat, gdzie wszyscy podlegaliby totalnemu nadzorowi, musiałby być rzeczywistością, w jakiej wszystkie obowiązujące prawa i przepisy byłyby egzekwowane przez

komputery w sposób totalny i automatyczny. Trudno bowiem wyobrazić sobie, by urządzenie wyposażone w sztuczną inteligencję i zdolne wyłuskać każdą osobę łamiącą prawo nie pociągnęło takiego człowieka do odpowiedzialności. W żaden nadzorujący algorytm nie zostałyby przecież wpisane – choćby nawet było to możliwe – pobłażliwość czy przymykanie oka.

Zastanawiałem się, czy nie byłoby to pełne, choć groteskowe urzeczywistnienie zawartej w amerykańskiej konstytucji zasady, że wszyscy obywatele są równi wobec prawa: egzekwowanie prawa w sposób totalny i automatyczny sprawiłoby, że wszyscy w równym stopniu stalibyśmy się ofiarami opresyjności systemu. Wyobrażałem sobie, że w przyszłości w mojej kuchni mogłaby stanąć „inteligentna lodówka", która monitorowałaby moje zachowania i nawyki, takie jak niemycie rąk czy picie soku prosto z kartonu, i oceniałaby na tej podstawie prawdopodobieństwo popełnienia przeze mnie jakiegoś poważnego przestępstwa.

Życie w świecie, w którym każde prawo – łącznie z przepisami zagospodarowania przestrzennego regulującymi prowadzenie działalności gospodarczej we własnym domu – byłoby egzekwowane totalnie i automatycznie, stałoby się nie do zniesienia. Absolutna sprawiedliwość może okazać się absolutną niesprawiedliwością; nie tylko za sprawą surowości kar za naruszenie prawa, ale także tego, z jak żelazną konsekwencją ścigane są te naruszania. W każdym społeczeństwie istnieje wiele niepisanych zasad, których przestrzegania oczekuje się od każdego jego członka, jak również wiele praw pisanych, których przestrzegania nikt od nas nie wymaga i z których istnienia często nawet nie zdajemy sobie sprawy. Według paragrafu 10-501 kodeksu karnego stanu Maryland przestępstwem jest cudzołóstwo; podlega ono karze grzywny w wysokości

dziesięciu dolarów. W Karolinie Północnej wciąż obowiązuje ustawa 14-309.8, zgodnie z nią sesja gry w bingo nie może trwać dłużej niż pięć godzin. Oba te przepisy pochodzą z dawnych, znacznie bardziej purytańskich czasów, a jednak z jakichś względów nigdy nie zostały uchylone. Nawet jeśli nie jesteśmy tego świadomi, nasze życie w większości nie jest ani czarne, ani białe; przybiera różne odcienie szarości – zdarza nam się przechodzić przez jezdnię w niedozwolonych miejscach, wrzucać nieposegregowane śmieci do pojemników na surowce wtórne, jeździć rowerem po chodniku zamiast po wyznaczonej ścieżce, korzystać z cudzego Wi-Fi, żeby ściągnąć z sieci książkę, choć za nią nie zapłaciliśmy. Krótko mówiąc, świat, w którym każdy przepis byłby zawsze i bezwzględnie egzekwowany, to rzeczywistość, gdzie każdy z nas byłby przestępcą.

Próbowałem porozmawiać o tym z Lindsay. Odniosła się do moich obaw ze zrozumieniem, ale nie zamierzała zaprzestać korzystania z sieci, ani nawet rezygnować z Facebooka czy Instagrama.

– Gdybym to zrobiła – stwierdziła – musiałabym pożegnać się z moją sztuką i z moimi przyjaciółmi. Poza tym przecież sam lubiłeś utrzymywać kontakty z innymi ludźmi.

Miała rację. Słusznie też się o mnie martwiła. Uważała, że jestem zbyt spięty, że żyję w zbyt dużym stresie. I rzeczywiście tak było – tyle tylko, że napięcie nie było wywołane pracą, ale chęcią wyznania Lindsay całej prawdy, której nie wolno mi było wyznać. Nie mogłem jej uprzedzić, że moi byli współpracownicy z NSA mogli uczynić ją obiektem inwigilacji i przeczytać miłosne wiersze, jakie wysyłała do mnie w SMS-ach. Nie wolno mi było powiedzieć jej o tym, że ludzie z NSA mogli uzyskać dostęp do wszystkich zrobionych przez nią zdjęć – nie tylko do udostępnionych publicznie, ale także do tych najbardziej osobistych. Nie mogłem zdradzić,

że zbierane są wszystkie informacje, które zamieszcza w sieci, że to samo dotyczy każdego z nas i że kryje się za tym niewypowiedziana groźba ze strony władz: jeśli kiedyś się nam narazisz, wykorzystamy twoje prywatne życie przeciw tobie.

Próbowałem wyjaśnić jej to nie wprost, posługując się analogią. Poprosiłem, by wyobraziła sobie, że pewnego dnia otwiera laptop i znajduje na pulpicie plik arkusza kalkulacyjnego.

– Niby po co? – odparła. – Nie lubię arkuszy kalkulacyjnych.

Nie spodziewałem się takiej reakcji, dlatego powiedziałem pierwsze, co przyszło mi do głowy.

– Nikt ich nie lubi, ale ten plik nazywa się „Koniec”.

– O, to brzmi tajemniczo.

– To nie ty utworzyłaś ten plik, ale kiedy go otwierasz, natychmiast rozpoznajesz zawartość. Bo jest tam wszystko, absolutnie wszystko, co mogłoby cię zniszczyć. Wszystkie informacje, które mogłyby zrujnować ci życie.

Lindsay uśmiechnęła się.

– A mogłabym zobaczyć twoją wersję takiego arkusza?

Żartowała sobie, ale mnie wcale nie było do śmiechu. Dokument zawierający wszystkie dane na twój temat może być śmiertelnie niebezpieczny. Pomyśl tylko: wszystkie duże i małe sekrety, których ujawnienie mogłoby zniszczyć ci małżeństwo i karierę, zatruć relacje ze wszystkimi bliskimi ci ludźmi i sprawić, że zostałbyś bez grosza przy duszy, bez przyjaciół, a może nawet wylądowałbyś za kratkami. Mogłaby się tam znaleźć informacja o skręcie, którego wypaliłeś w zeszły weekend w mieszkaniu znajomego, albo o kresce kokainy wciągniętej przez ciebie z ekranu telefonu podczas imprezy w barze jeszcze na studiach. Albo o jednorazowej przygodzie z dziewczyną twojego przyjaciela, dziś jego

żoną – choć oboje tego żałujecie i zgodziliście się nigdy nikomu o tym nie wspominać. Albo o aborcji, której poddałaś się jako nastolatka; nie powiedziałaś o niej rodzicom i nie chciałabyś, żeby dowiedział się o niej twój mąż. Albo o podpisanej petycji lub o manifestacji, w której wziąłeś udział. Każdy z nas ma jakiś sekret, kompromitujące go informacje, zakopane gdzieś pośród niezliczonych bajtów danych – jeśli nie w jednym z plików, to w którymś z e-maili, jeśli nie w e-mailu, to w historii przeglądanych stron. A teraz te dane znajdują się w rękach rządu Stanów Zjednoczonych.

Jakiś czas po tamtej rozmowie Lindsay podeszła do mnie i powiedziała:

– Już wiem, co znalazłoby się w moim Arkuszu Totalnego Zniszczenia. Sekret, który by mnie zniszczył.

– Czyli?

– Nie powiem.

Próbowałem się odprężyć, ale zaczęły trapić mnie dziwne fizyczne objawy. Stałem się wyraźnie niezdarny: spadłem z drabiny – więcej niż raz – i obijałem się o framugi drzwi. Potykałem się, upuszczałem na podłogę łyżki albo niewłaściwie oceniałem dystans dzielący mnie od różnych przedmiotów i kiedy wyciągałem po nie rękę, trafiałem dłonią w próżnię. Zdarzało mi się oblać siebie wodą ze szklanki albo zakrztusić się podczas picia. W trakcie rozmów z Lindsay umykało mi czasem to, co do mnie mówiła; pytała, gdzie błądzę myślami, a ja nie potrafiłem jej odpowiedzieć – czułem się, jakbym zamarł i na chwilę trafił do innego świata.

Któregoś dnia spotkałem się z Lindsay po jej zajęciach fitnessu na rurze. Niespodziewanie zakręciło mi się w głowie. To był najbardziej niepokojący z dotychczasowych objawów. Napędził nam obojgu stracha, zwłaszcza że po zawrotach głowy doświadczyłem stopniowego

przytępienia zmysłów. Miałem wytłumaczenie dla tych wszystkich incydentów: kiepska dieta, brak ruchu, niedostatek snu. Próbowałem racjonalizować przydarzające mi się wypadki: wmawiałem sobie, że talerz był zbyt blisko krawędzi blatu, a schody – śliskie. Sam nie wiedziałem, co byłoby gorsze – psychosomatyczne czy fizjologiczne tło moich dolegliwości. W końcu postanowiłem udać się do lekarza, ale najbliższy wolny termin wypadał dopiero za kilka tygodni.

Dzień lub dwa dni po wystąpieniu pierwszych zawrotów głowy zostałem w domu i próbowałem pracować zdalnie. Było południe, rozmawiałem przez telefon z dyrektorem Della do spraw bezpieczeństwa, gdy nagle mocno zakręciło mi się w głowie. Natychmiast zakończyłem rozmowę, mamrocząc bełkotliwie słowa przeprosin. Próbowałem odłożyć słuchawkę telefonu. Byłem pewien, że za chwilę umrę.

Tym, którzy sami tego doświadczyli, nie trzeba opisywać tego przeczucia nieuchronnie zbliżającej się śmierci. Pozostałym nie da się go wyjaśnić ani opisać. Przychodzi nagle i uderza z taką pierwotną siłą, że zagłusza wszelkie inne odczucia i wrażenia, wypiera każdą myśl, pozostawiając poczucie bezsilnej rezygnacji. Moje życie dobiegało końca. Opadłem na fotel. Duży, czarny, wyścielany mebel marki Aeron ugiął się pode mną, a ja poczułem, że spadam w otchłań, i zemdlałem.

Odzyskałem przytomność, siedząc na fotelu. Spojrzałem na zegar – dochodziła pierwsza po południu. Byłem nieprzytomny przez niespełna godzinę, ale czułem się potwornie wyczerpany. Miałem wrażenie, że nie zmrużyłem oka od początku świata.

Ogarnięty paniką sięgnąłem po telefon, ale nie byłem w stanie odnaleźć dłonią słuchawki. W końcu mi się udało. Kiedy usłyszałem w słuchawce ciągły sygnał, zdałem sobie sprawę, że nie potrafię sobie przypomnieć

numeru komórki Lindsay. Pamiętałem poszczególne cyfry, jednak nie byłem w stanie ich uporządkować.

Jakimś cudem udało mi się zejść po schodach na parter. Stawiałem ostrożnie każdy krok, opierając się ręką o ścianę. Kiedy dotarłem do kuchni, wyciągnąłem z lodówki karton soku i trzymając go oburącz, zacząłem łapczywie pić. Spora część płynu zamiast trafić do ust, popłynęła mi po brodzie. Potem położyłem się na podłodze, oparłem policzek o chłodne linoleum i zasnąłem. Śpiącego na kuchennej posadzce znalazła mnie po powrocie do domu Lindsay.

Miałem napad padaczkowy.

Moja mama cierpiała na padaczkę i przez pewien czas występowały u niej poważne ataki: na jej ustach pojawiała się piana, kończynami targały silne drgawki, a całe jej ciało przetaczało się po podłodze, po czym ulegało okropnemu zesztywnieniu, połączonemu z utratą świadomości. Nie mogłem uwierzyć, że nie skojarzyłem z tym moich wcześniejszych objawów. Najwyraźniej wypierałem ze świadomości tę chorobę, tak samo jak moja mama, która przez kilka dekad z uporem przypisywała częste upadki „niezdarności” i „kiepskiej koordynacji”. Padaczkę zdiagnozowano u niej dopiero po pierwszym poważnym napadzie, kiedy dobiegała już czterdziestki. Po krótkiej kuracji lekowej ataki ustąpiły. Mama zawsze przekonywała mnie i moją siostrę, że padaczka nie jest chorobą dziedziczną – do dziś nie jestem pewien, czy tak powiedział jej lekarz, czy może po prostu chciała nas przekonać, że nie jesteśmy skazani na ten sam los, co ona.

Nie ma testów diagnostycznych, które pozwoliłyby rozpoznać padaczkę przed wystąpieniem objawów. Diagnozę stawia się na podstawie dwóch lub więcej epizodów – to wszystko. Na temat samej choroby wciąż wiadomo stosunkowo niewiele. Medycyna podchodzi do niej w sposób

fenomenologiczny, opierając diagnostykę i tryb leczenia na wywiadzie z pacjentem, opisach napadów oraz towarzyszących im okoliczności. Lekarze nie mówią o „padaczce”, tylko o „napadach padaczkowych”. Dzielą je na dwie kategorie: ogniskowe i rozproszone. Napady ogniskowe powodowane są przez nadmierne wyładowania elektryczne w określonej części mózgu, które nie rozprzestrzeniają się dalej. W przypadku napadów rozproszonych wyładowanie elektryczne zapoczątkowuje reakcję łańcuchową obejmującą cały mózg i prowadzącą do zaburzenia funkcji ruchowych, a następnie do utraty świadomości.

Padaczka to bardzo dziwna choroba. Cierpiący na nią doświadczają rozmaitych zaburzeń i objawów w zależności od tego, gdzie w ich mózgu znajduje się ognisko padaczkowe. Ci, u których znajduje się ono w ośrodku słuchu, słyszą często bicie dzwonów. Ci, u których do wyładowań dochodzi w ośrodku wzroku, widzą błyski lub ciemność. Jeśli do nadmiernych wyładowań dochodzi w głębiej położonych obszarach kory mózgu – tak jak miało to miejsce w moim przypadku – chory doświadcza silnych zawrotów głowy. Z czasem nauczyłem się rozpoznawać sygnały ostrzegawcze i mogłem przygotować się na nadciągający napad. Zwiastujące atak objawy nazywa się potocznie „aurą”, chociaż z naukowego punktu widzenia są one częścią samego napadu. To proprioceptywne doświadczanie wyładowań bioelektrycznych, do jakich dochodzi w komórkach nerwowych mózgu.

Skonsultowałem się z tyloma specjalistami od padaczki, ilu tylko udało mi się znaleźć. Najlepsze w pracy w Dellu było ubezpieczenie medyczne: dzięki niemu mogłem przejść tomografię komputerową, rezonans magnetyczny, pełen zestaw badań. Lindsay oprócz tego, że dzielnie woziła mnie na wszystkie badania i wizyty u specjalistów, szukała także na własną rękę wszelkich dostępnych informacji na temat mojej choroby. Niestrudzenie wyszukiwała w Google’u rozmaite leki homeopatyczne

i alopatyczne, aż w końcu niemal wszystkie reklamy, jakie pojawiały się w jej skrzynce gmailowej, dotyczyły leków przeciwpadaczkowych.

Czułem się pokonany. Dwie najważniejsze instytucje mojego życia – kraj i internet – padły ofiarą zdrady i zdradziły mnie. A teraz dołączyło do nich także moje ciało.

W moim mózgu, całkiem dosłownie, nastąpiło zwarcie.

18_Na_sofie|

Późnym wieczorem 1 maja 2011 roku na ekranie mojego telefonu pojawiło się powiadomienie: Osama bin Laden został wytropiony w mieście Abbottabad w Pakistanie i zabity przez oddział komandosów z Navy SEALs.

A więc stało się. Pomysłodawca i organizator zamachów, które skłoniły mnie do zaciągnięcia się do wojska, a potem do wstąpienia do służb wywiadowczych, był martwy. Osama bin Laden, chorujący na nerki i wymagający regularnych dializ, został zabity strzałem z bliska na oczach licznych żon, z którymi ukrywał się w okazałej, ufortyfikowanej posiadłości nieopodal siedziby pakistańskiej akademii wojskowej. Na stronach serwisów informacyjnych pokazywano na przemian mapki z zaznaczonym Abbottabadem i sceny rozgrywające się na ulicach amerykańskich miast – mieszkańcy zaciskali triumfalnie pięści, stukali się klatami, krzyczeli i upijali się z radości. Nawet Nowy Jork świętował, co nie zdarza się zbyt często.

Wyłączyłem telefon.

Nie miałem ochoty przyłączać się do tej fiesty.

Nie zrozum mnie źle: cieszyłem się, że skurwiel nie żyje. Po prostu ogarnął mnie refleksyjny nastrój i poczucie, że znalazłem się w punkcie wyjścia.

Dziesięć lat. Tyle minęło od dnia, gdy dwa porwane samoloty uderzyły w bliźniacze wieże World Trade Center – i co przez ten czas osiągnęliśmy? Czego udało nam się dokonać? Siedziałem na starej sofie, która trafiła do

mnie z mieszkania mamy, i spoglądałem przez okno na ulicę, gdzie jeden z sąsiadów wsiadł do zaparkowanego przed domem samochodu i trąbił klaksonem. Nie mogłem oprzeć się wrażeniu, że zmarnowałem dziesięć lat życia.

Mijająca dekada była pasmem sprokurowanych przez Amerykę nieszczęść: niekończąca się wojna w Afganistanie, katastrofalna w skutkach zmiana reżimu w Iraku, bezterminowe przetrzymywanie więźniów w obozie Guantanamo, procesy w trybie nadzwyczajnym, tortury, używanie dronów do selektywnej eliminacji cywilów, w tym także obywateli Stanów Zjednoczonych. To za granicą. U nas w kraju tymczasem następowało zwiększanie uprawnień Departamentu Bezpieczeństwa Krajowego, który ingerował we wszystkie dziedziny życia i każdego dnia określał stopień zagrożenia terrorystycznego (czerwony – najwyższy, pomarańczowy – wysoki, żółty – podwyższony); po uchwaleniu ustawy Patriot Act* rozpoczęło się systematyczne ograniczanie swobód obywatelskich, tych samych swobód, których mieliśmy rzekomo bronić. Ogrom szkód – efekty wszystkich nadużyć władzy – był porażający, a dokonujące się zmiany wydawały się nieodwracalne; tymczasem w radosnym uniesieniu trąbiliśmy klaksonami i błyskaliśmy światłami.

Największy w historii atak terrorystyczny, jaki wydarzył się na amerykańskiej ziemi, zbiegł się w czasie z dynamicznym rozwojem technologii cyfrowych, przez co amerykańską ziemią stała się większość świata – czy nam się to podoba, czy nie. W okresie wielkiego strachu i oportunizmu, jaki nastał po wydarzeniach 11 września 2001 roku, oficjalnym powodem wprowadzenia w naszym kraju programów masowej inwigilacji było zagrożenie ze strony terrorystów. Jak się jednak okazało, prawdziwym terrorystą był strach, podsycany przez przedstawicieli amerykańskiego systemu politycznego, gotowych wykorzystać dowolny

pretekst do wydania zgody na użycie siły. Amerykańscy politycy obawiali się nie tyle terroru, co okazania słabości, a także nielojalności wobec własnej partii oraz wobec sponsorów kampanii wyborczych, którzy mieli chrapkę na rządowe kontrakty i bliskowschodnią ropę. Polityczna odpowiedź na akt terroru okazała się bardziej destrukcyjna niż sam akt i poskutkowała „walką z terroryzmem": panicznymi działaniami państwa dysponującego niezrównanym potencjałem, nieskrępowanego politycznymi uwarunkowaniami i ewidentnie niedbającego o zachowanie zasad praworządności. Po 11 września 2001 amerykańskim agencjom wywiadowczym rozkazano dopilnować, by Ameryka „nigdy więcej" nie padła ofiarą zamachu; było to oczywiście zadanie absolutnie niewykonalne. Dziesięć lat później stało się jasne, przynajmniej dla mnie, że ciągłe epatowanie zagrożeniem terrorystycznym przez członków naszej klasy politycznej nie było reakcją na żadne konkretne przesłanki wskazujące na ryzyko kolejnego ataku, tylko cyniczną próbą wywołania w społeczeństwie poczucia permanentnego niebezpieczeństwa, wymagającego nieustannej czujności i zdecydowanych kroków władzy, której poczynań nikt nie ośmieli się kwestionować.

Dekada masowej inwigilacji dowiodła, że nowoczesna technologia jest niezwykle skuteczną bronią, nie tyle jednak przeciwko terroryzmowi, co przeciw wolności. Kontynuując programy masowej inwigilacji i brnąc dalej w kłamstwa, Ameryka niewiele chroniła, niczego nie wygrywała, za to wiele traciła. Coraz bardziej zacierały się różnice we wprowadzonym po 11 września podziale na „Nas" i na „Nich".

Druga połowa 2011 roku upłynęła mi pod znakiem powtarzających się ataków padaczkowych oraz niezliczonych wizyt w szpitalach i gabinetach lekarskich. Przeszedłem badania obrazowe i testy, po czym przepisano mi

leki; te ustabilizowały stan mojego ciała, ale zamroczyły mój umysł: stałem się przygnębiony, apatyczny i miałem problemy z koncentracją.

Nie wiedziałem, jak pogodzić to, co Lindsay nazywała moją „przypadłością", z pracą zawodową. Jako wysoki rangą specjalista do spraw technologii, oddelegowany przez Della do CIA, miałem wolną rękę w wyborze miejsca pracy: moim biurem był telefon i mogłem z powodzeniem wypełniać obowiązki z domu. Problemem były zebrania i spotkania służbowe. Wszystkie odbywały się w Wirginii, a ja mieszkałem w Marylandzie. Obowiązujące w tym stanie przepisy zabraniały prowadzenia samochodu osobom, u których zdiagnozowano epilepsję; gdyby przyłapano mnie za kierownicą, straciłbym prawo jazdy, a wraz z nim możliwość udziału w zebraniach – była to jedyna rzecz, na jaką nie mogłem sobie pozwolić na moim stanowisku.

W końcu dałem za wygraną i pogodziłem się z nieuniknionym. Wziąłem krótkoterminowy urlop z przyczyn zdrowotnych i zakotwiczyłem na dobre na naszej starej sofie. Granatowy odcień jej obicia był równie ponury, co mój nastrój, ale nie można było odmówić meblowi wygody. Na wiele tygodni sofa stała się centrum mojej egzystencji – na niej spałem, jadłem, czytałem i znowu spałem; tam też, pogrążony w posępnym stuporze, starałem się zabić złośliwie wolno płynący czas.

Nie potrafię sobie przypomnieć, jakie książki próbowałem wtedy czytać, ale pamiętam, że nigdy nie udawało mi się przebrnąć przez więcej niż jedną stronę naraz – potem opadały mi powieki i zapadałem się w miękkie poduszki. Nie byłem w stanie skupić się na niczym poza własną słabością. Zobojętniały na wszelkie bodźce, leżałem na sofie niczym kloc, w niemal zupełnym bezruchu, nie licząc palca przesuwającego się po ekranie telefonu – jedynym źródle światła w ciemnym pokoju.

Przeglądałem strony serwisów informacyjnych, zapadałem w drzemkę, po przebudzeniu się znowu wodziłem palcem po ekranie smartfona, a potem znowu zaczynałem drzemać. W tym samym czasie demonstranci w Tunezji, Libii, Egipcie, Jemenie, Algierii, Maroku, Iraku, Libanie i Syrii byli wtrącani do więzień i torturowani albo ginęli na ulicach od kul agentów tajnej policji, wypełniających rozkazy bezwzględnych dyktatorów, z których wielu utrzymywało się przy władzy dzięki amerykańskiemu wsparciu. Cierpienie, jakie było udziałem protestujących, wykraczało daleko poza to, do czego przyzwyczaiły nas codzienne artykuły w mediach. Byłem świadkiem aktów desperacji, przy których moje problemy wydawały się powierzchowne. Zdawały się trywialne – pod względem etycznym i moralnym – i typowe dla uprzywilejowanych ludzi Zachodu.

Niewinni mieszkańcy większości bliskowschodnich krajów żyli w stanie nieustannego zagrożenia przemocą; zamknięto szkoły i zakłady pracy, odłączono prąd, nie działała kanalizacja. W wielu miejscach ludzie nie mieli dostępu do podstawowej opieki medycznej. Jeśli kiedykolwiek miałem wątpliwości co do tego, czy moje obawy związane z inwigilacją i naruszaniem prawa do prywatności były uzasadnione – a nawet czy nie były niestosowne w zestawieniu z bezpośrednim zagrożeniem życia i fatalnymi warunkami egzystencji mieszkańców Bliskiego Wschodu – to wystarczyło, że przyjrzałem się uważniej hasłom i proklamacjom uczestników protestów na ulicach Kairu i Sany, Bejrutu i Damaszku, Ahwazu i każdego innego miasta, które ogarnęła arabska wiosna lub irańska zielona rewolucja. Wszędzie domagano się położenia kresu uciskowi, zniesienia cenzury oraz poprawy warunków życia. Demonstranci przypominali, że w prawdziwie sprawiedliwym społeczeństwie to władza powinna odpowiadać przez narodem, a nie naród przed władzą. Chociaż w każdym miejscu protestujący mieli własne, specyficzne motywy i cele,

nierzadko zmieniające się z dnia na dzień, to było też coś, co ich wszystkich łączyło: odrzucenie autorytaryzmu i uznanie zasady, że prawa jednostki są przyrodzone i niezbywalne.

W państwie autorytarnym wszelkie prawa, które posiadają i którymi kierują się jego obywatele, pochodzą od władzy i to władza przyznaje je narodowi. W demokratycznym państwie prawo pochodzi od narodu i to naród udziela władzy prawa do rządzenia. W państwie autorytarnym człowiek podlega władzy w wielu aspektach życia: może posiadać majątek, kształcić się, pracować, modlić i zabierać publicznie głos tylko dlatego, że pozwala mu na to ten, kto sprawuje władzę. W państwie demokratycznym ludzie są obywatelami i to zgoda obywateli na bycie rządzonymi stanowi podstawę sprawowania władzy przez odpowiednie instytucje; zgoda ta musi być systematycznie odnawiana i może być cofnięta w określony w konstytucji sposób. Jestem przekonany, że to właśnie między autorytaryzmem a demokracją liberalną rozgrywa się zasadniczy konflikt naszych czasów – jest to rzeczywista oś sporu, w przeciwieństwie do wyimaginowanych, takich jak wynikające z uprzedzeń koncepcje ścierania się Wschodu i Zachodu czy świata chrześcijańskim i świata islamu.

W państwach autorytarnych zwykle nie panują rządy prawa, lecz rządy jednostki: przywódcy, który wymaga od społeczeństwa całkowitej lojalności i wrogo odnosi się do wszelkich przejawów odmienności poglądów. Państwa liberalno-demokratyczne nie domagają się od obywateli lojalności w tak wielu aspektach życia i polegają przede wszystkim na dobrowolnym przyjęciu przez każdego obywatela odpowiedzialności za stanie na straży wolności innych, niezależnie od ich rasy, tożsamości etnicznej, wyznania, zdolności, orientacji seksualnej czy płci. Każda wspólnota mająca za cel realizację zbiorowych gwarancji, o ile nie jest oparta na pokrewieństwie, tylko na umowie członków, będzie preferować

egalitaryzm jako zasadę organizacji stosunków pomiędzy swoimi członkami. I chociaż realizacje ustroju demokratycznego często odbiegają od ideału, to wierzę, że ta forma rządów lepiej niż jakakolwiek inna pozwala ludziom wywodzącym się z różnych środowisk żyć razem w równości wobec prawa.

Ta równość dotyczy nie tylko praw, ale i wolności. Wiele zasad szczególnie drogich obywatelom państw demokratycznych to prawa dorozumiane – nie zostały one zapisane wprost w ustawach ani innych aktach prawnych. Istnieją dzięki ustrojowym ograniczeniom władzy państwowej. Przykładowo obywatele Stanów Zjednoczonych mają prawo do wolności wyrażania opinii, ponieważ władza nie może wydawać żadnych aktów prawnych ograniczających wolność słowa; mają prawo do wolności prasy, gdyż władza nie może go zakazywać; mają prawo do wolności wyznania, bo władza nie może ustanawiać żadnych praw wprowadzających religię ani zabraniających wykonywania praktyk religijnych, a także posiadają prawo do pokojowych zgromadzeń i protestów, ponieważ władza nie może stanowić ustaw, które by im tego zabraniały.

Współcześnie dysponujemy jednym pojęciem obejmującym wszystkie te wolności czy też obszary życia, w które nie może ingerować władza państwowa. Tym pojęciem jest prywatność. To wolna strefa, leżąca poza zasięgiem państwa; przestrzeń, do której organy państwa mogą uzyskać dostęp wyłącznie na podstawie nakazu. I to nie nakazu w stosunku „do każdego” – takiego jak ten, który przyznał sobie rząd Stanów Zjednoczonych, by realizować swoje programy masowej inwigilacji – ale nakazu wydanego w odniesieniu do konkretnej osoby i tylko w sytuacji, gdy istnieją uzasadnione podstawy do jego wydania.

Słowo „prywatność” jest w pewnym sensie pojęciem pustym, ponieważ nie da się go jednoznacznie zdefiniować – choć może należałoby raczej powiedzieć, że istnieje zbyt wiele możliwych jego definicji. Wszyscy mamy swoje własne wyobrażenia o tym, czym jest „prywatność”. Termin ten dla każdego z nas coś oznacza. Nie ma osoby, dla której nie znaczyłby zupełnie nic.

To między innymi za sprawą tego braku jednoznacznej definicji obywatele pluralistycznych, zaawansowanych technologicznie demokracji mają poczucie, że muszą jakoś uzasadnić swoje pragnienie zachowania prywatności i ująć je w formie prawa. W rzeczywistości jednak wcale nie muszą tego robić – to władza musi uzasadnić pogwałcenie prywatności obywatela.

Prywatności nie da się po prostu zignorować. Ponieważ wolności obywatelskie są współzależne, zrzeczenie się prywatności oznacza rezygnację z prywatności wszystkich twoich współobywateli. Możesz wyrzec się prywatności z wygody lub ulegając obiegowej opinii, że prywatność potrzebna jest tylko tym, którzy mają coś do ukrycia. Ale stwierdzając, że prywatność nie jest ci potrzebna, ponieważ nie masz nic do ukrycia, zakładasz jednocześnie, że inni ludzie również nie mają, a przynajmniej nie powinni mieć niczego do ukrycia – wliczając w to ich status imigracyjny, historię finansową czy informacje o stanie zdrowia i przebytych chorobach. Zakładasz, że nikt, łącznie z tobą, nie będzie miał nic przeciwko ujawnieniu informacji na temat swoich przekonań religijnych, sympatii politycznych czy aktywności seksualnej i że każdy powinien podchodzić do tego równie beztrosko, jak do ujawnienia preferencji muzycznych czy literackich.

Oświadczyć, że nie obchodzi cię prywatność, bo nie masz nic do ukrycia, to mniej więcej to samo, co oświadczyć, że nie obchodzi cię

wolność słowa, ponieważ nie masz nic do powiedzenia. Albo że nie dbasz o wolność prasy, bo nie czytasz gazet. Albo że wolność wyznania nie ma dla ciebie znaczenia, bo nie wierzysz w Boga. Albo że nie interesuje cię wolność pokojowych zgromadzeń, bo jesteś gnuśnym aspołecznym agorafobem. Nawet jeśli dana wolność nie ma dla ciebie znaczenia dziś, może okazać się ważna jutro, jeżeli nie dla ciebie, to dla twojego sąsiada – albo dla tłumów ludzi, które wyległy na ulice na drugim końcu świata w nadziei na to, że uda im się wywalczyć choćby cząstkę tych wolności, jakie mój kraj właśnie zawzięcie likwidował.

Chciałem im jakoś pomóc, ale nie miałem pojęcia, jak mógłbym to zrobić. Wiedziałem tylko, że mam już serdecznie dość poczucia bezsilności; nie chciałem już dłużej być dupkiem we flanelowej koszuli, wylegującym się na sfatygowanej kanapie, wcinającym czipsy Cool Ranch Doritos i popijającym dietetyczną colę, kiedy świat stoi w płomieniach.

Młodzi z Bliskiego Wschodu domagali się wyższych płac, niższych cen, lepszego systemu emerytalnego. Nie mogłem zapewnić im żadnej z tych rzeczy. Nie byłem w stanie również dać im większej szansy na wywalczenie prawa do współdecydowania o losach swojego kraju niż ta, którą sami sobie stworzyli, wychodząc na ulice. Ale wśród postulatów uczestników arabskiej wiosny i zielonej rewolucji znalazło się również hasło większej swobody w dostępie do internetu. W Iranie protestowano przeciwko poczynaniom Ajatollaha Chameneiego, który wprowadzał coraz bardziej restrykcyjną kontrolę dostępu do sieci, blokował dostęp do nieprawomyślnych treści, hakował niepodporządkowujące się cenzurze platformy i portale, a także zamykał działające na terenie Iranu oddziały zagranicznych firm, zajmujące się dostarczaniem usług internetowych. W Egipcie protestowano przeciwko prezydentowi Mubarakowi, który odciął dostęp do internetu w całym kraju – czym jeszcze bardziej

rozsierdził wszystkich młodych ludzi i skłonił ich do przyłączenia się do protestów.

Odkąd podczas pobytu w Genewie zapoznałem się z projektem Tor, korzystałem z niego do przeglądania stron internetowych; uruchomiłem też własny serwer Tor, żeby móc pracować z domu bez narażania się na to, że padnę ofiarą cyberszpiegostwa. Teraz otrząsnąłem się z apatii, wstałem z kanapy i chwiejnym krokiem udałem się do mojego domowego biura, żeby uruchomić serwer pośredniczący, który pozwoliłby irańskim internautom obejść rządowe blokady i połączyć się z siecią Tor. Następnie przesłałem zaszyfrowaną identyfikację konfiguracji mojego serwera programistom Tora.

Przynajmniej tyle mogłem zrobić. Jeśli istniała najmniejsza nawet szansa, że jakiś dzieciak z Iranu, który nie mógł wejść do sieci, zdoła teraz objeść rządowe filtry i połączy się ze mną – i za moim pośrednictwem z siecią – chroniony przez system Tor i anonimowość, jaką zapewniał mu mój serwer, to z pewnością było to warte odrobiny wysiłku, jaki musiałem w to włożyć.

Wyobraziłem sobie tę osobę, czytającą e-maile albo logującą się na swoje konto w mediach społecznościowych, żeby upewnić się, czy jej bliscy i przyjaciele nie zostali aresztowani. Rzecz jasna nie wiedziałem, czy ktoś to zrobił ani nawet czy ktokolwiek połączył się z Iranu z moim serwerem. I o to w tym chodziło: pomoc, jakiej udzieliłem, była ściśle prywatna.

Gość, który dał początek arabskiej wiośnie, był niemal w moim wieku. Był ulicznym handlarzem z Tunezji, sprzedającym owoce i warzywa z wózka. Na znak protestu przeciw ciągłemu nękaniu go przez policję i wymuszaniu łapówek podpalił się na środku placu i zginął męczeńską śmiercią. Jeśli on zdecydował się na samospalenie w ostatnim akcie wolnej

woli oraz sprzeciwu wobec bezprawnego reżimu, to ja z pewnością mogłem zwlec tyłek z kanapy i nacisnąć kilka klawiszy.

---

* Potoczna nazwa ustawy uchwalonej w 2001 w konsekwencji zamachów z 11 września – USA PATRIOT Act (akronim od Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Jednoczenie i Wzmacnianie Ameryki przez Zapewnianie Stosownych Narzędzi do Przechwytywania i Utrudniania Działań Terrorystycznych) (przyp. red).

Część_03|

19_Tunel|

Wyobraź sobie, że wchodzisz do tunelu. Przed sobą masz ciągnące się w dal ściany, które zbiegają się do niewielkiej plamki światła. Światełko w tunelu to symbol nadziei; widzą je także osoby w stanie śmierci klinicznej. Opowiadają, że czuły przymus, by dążyć ku niemu, jakby je przyciągało. Z drugiej strony, kiedy już znajdziesz się w tunelu, dokąd miałbyś się kierować? Przecież wszystko doprowadziło cię właśnie tutaj…

Moim tunelem okazał się Tunel – tak właśnie nieoficjalnie nazywano bazę NSA utworzoną w ogromnej fabryce samolotów z czasów Pearl Harbor, zlokalizowaną pod polami ananasów w Kunii na wyspie Oahu na Hawajach. Obiekt zbudowano z żelbetu, a tunel, od którego wziął swoją nazwę, ciągnie się na kilometr w głąb wzgórza i przechodzi w trzy rozległe poziomy serwerowni i biur. Podczas budowy Tunelu wzgórze pokryto dużą ilością piasku, gleby, zeschłych liści ananasów oraz połaciami spalonej słońcem trawy, by ukryć je przed załogami japońskich bombowców. Sześćdziesiąt lat później przypominało ono wielki kurhan wymarłej cywilizacji lub gigantyczny stos zeschłych resztek usypany przez pomylonego boga w należącej do niego piaskownicy. Oficjalnie placówka nosiła nazwę Kunia Regional Security Operations Center (Regionalny Ośrodek Operacji Bezpieczeństwa w Kunii).

Rozpocząłem tam pracę na początku 2012 roku, nadal związany umową z firmą Dell, ale teraz znów wykonując zadania dla NSA. Pewnego dnia latem tamtego roku – a dokładniej w moje urodziny – kiedy po przejściu

kontroli bezpieczeństwa podążałem Tunelem, uderzyło mnie nagle, że tam, przede mną, znajduje się moja przyszłość.

Nie twierdzę, że właśnie wtedy podjąłem decyzję. Najważniejszych życiowych decyzji nigdy nie podejmuje się w taki sposób. Dojrzewają one stopniowo w podświadomości, a formułujemy je świadomie dopiero wówczas, kiedy przyjmą ostateczny kształt – gdy nabierzesz dość siły, żeby przyznać przed sobą, że twoje sumienie i przekonania już wybrały dla ciebie tę drogę. Moim prezentem dla siebie na dwudzieste dziewiąte urodziny było uświadomienie sobie, że wkroczyłem do tunelu, który zawęzi moje życie do pojedynczego, na razie niesprecyzowanego jeszcze czynu.

Hawaje zawsze były ważnym punktem przerzutowym; amerykańskie wojsko wykorzystywało tę lokalizację głównie jako bazę zaopatrzeniową na Pacyfiku, gdzie okręty i samoloty uzupełniają paliwo. Teraz stała się dodatkowo ważnym amerykańskim węzłem łączności. Przepływały tamtędy między innymi informacje wywiadowcze przesyłane pomiędzy sąsiadującymi ze sobą czterdziestoma ośmioma stanami USA a moim dawnym miejscem zatrudnienia, czyli Japonią, oraz innymi częściami Azji.

Praca, którą podjąłem, była sporym krokiem wstecz w mojej karierze zawodowej, mogłem więc wykonywać ją niemal z zamkniętymi oczami. Zdecydowałem się na nią dlatego, że oznaczała dla mnie mniej obciążenia i stresu. Byłem jedynym pracownikiem Biura Wymiany Informacji, gdzie pełniłem funkcję administratora systemów SharePoint. SharePoint to oferowane przez Microsoft głupawe i ślamazarne oprogramowanie, a raczej pakiet programów obsługujący zarządzanie wewnętrznymi dokumentami; pozwala ustalić, co komu wolno czytać, redagować, wysyłać lub odbierać i tak dalej. Kiedy NSA mianowała mnie administratorem systemu SharePoint na Hawajach, obsadziła mnie w istocie na stanowisku menedżera do spraw zarządzania dokumentami. W rezultacie stałem się

głównym recenzentem materiałów w jednym z najważniejszych ośrodków agencji. Jak to miałem w zwyczaju na każdym nowym technicznym stanowisku, zacząłem od zautomatyzowania zadań – czyli napisania skryptów, które miały za mnie wykonywać pracę – żeby zyskać czas na bardziej interesujące zajęcia.

Zanim przejdę dalej, chciałbym podkreślić jedno: nie rozpocząłem aktywnego wyszukiwania nadużyć NSA od kopiowania dokumentów, lecz od ich czytania. Początkowo chciałem się tylko przekonać, czy podejrzenia, które po raz pierwszy nasunęły mi się na myśl w 2009 roku w Tokio, były słuszne. Trzy lata później postanowiłem sprawdzić, czy amerykański system masowej inwigilacji w rzeczywistości istnieje, a jeśli tak, to jak funkcjonuje. Nie byłem jeszcze pewien, w jaki sposób przeprowadzić to śledztwo, ale jedno wiedziałem na pewno: muszę zrozumieć, jak to wszystko działa, zanim będę mógł zdecydować, co z tym zrobić, i czy w ogóle coś robić.

Oczywiście nie tylko dlatego trafiliśmy z Lindsay na Hawaje. Nie przeprowadzaliśmy się taki kawał drogi do raju tylko po to, żebym mógł zniszczyć nasze wspólne życie w imię wierności zasadom.

Przybyliśmy tu, żeby zacząć od nowa. Jeszcze raz.

Lekarze uznali, że hawajski klimat i swobodniejszy tryb życia będą korzystne dla mojego zdrowia. Że powinny pomóc w złagodzeniu padaczki, której napady wynikały, ich zdaniem, między innymi z braku snu. Poza tym pobyt na Hawajach rozwiązywał problem z prowadzeniem samochodu, bowiem z Kunii, spokojnego miejsca w samym środku suchego, czerwonego wnętrza wyspy, spokojnie można było dojechać do Tunelu rowerem. Odbywałem zatem przyjemną, dwudziestominutową przejażdżkę w słońcu przez pola trzciny cukrowej, napawając się widokiem pięknych

gór na horyzoncie. W takich warunkach ponury nastrój gnębiący mnie przez ostatnie miesiące rozproszył się wkrótce po przyjeździe jak poranna mgiełka.

Znaleźliśmy z Lindsay sporej wielkości bungalow przy Eleu Street w Royal Kunia pod Waipahu i umeblowaliśmy go tym, co przywieźliśmy z Columbii w Marylandzie, skoro Dell opłacał nam przeprowadzkę. Co prawda, okazało się, że nie mieliśmy wielkiego pożytku z tych mebli, bo przy panującym na wyspie upale często tuż po przekroczeniu drzwi zrzucaliśmy ubrania i kładliśmy się nago na dywanie pod dyszącym z wysiłku klimatyzatorem. Po pewnym czasie Lindsay zmieniła garaż w salę do fitnessu, rozłożyła w nim maty do jogi i ustawiła rurę obrotową, którą przywiozła z Columbii. Ja natomiast zainstalowałem tam serwer sieci Tor. Wkrótce informacje z całego świata przepływały do internetu przez laptop ustawiony w naszym centrum rekreacyjnym, co miało też taką zaletę, że maskowało moją własną internetową aktywność.

Pewnego letniego wieczoru, już po moich dwudziestych dziewiątych urodzinach, Lindsay w końcu uprosiła mnie, bym wybrał się z nią na luau. Przekonywała mnie już od pewnego czasu, bo kilka jej koleżanek, z którymi ćwiczyła fitness na rurze, tańczyło również hula. Odmawiałem, nie chcąc czuć się jak typowy turysta zaliczający miejscowe atrakcje; poza tym wydawało mi się, że uczestnicząc w imprezie, zademonstruję brak szacunku. Hawajczycy zakorzenieni są w pradawnej kulturze, którą nadal żywo kultywują, a ja nie chciałem zakłócać ich świętych rytuałów.

Ostatecznie jednak uległem i jestem z tego bardzo zadowolony. Główną część luau stanowił taniec z ogniem – naprawdę spektakularne widowisko – ale na mnie największe wrażenie zrobił starszy mężczyzna, który w małym amfiteatrze nad brzegiem morza zgromadził wokół siebie sporą grupę słuchaczy. Był Hawajczykiem przemawiającym charakterystycznym dla

mieszkańców tych wysp miękkim, nosowym głosem i opowiadał zebranym przy ognisku historie o stworzeniu świata przekazywane z pokolenia na pokolenie przez rdzenną ludność.

Najbardziej utkwiła mi w pamięci opowieść o dwunastu świętych wyspach bogów. Podobno na Pacyfiku istniało kiedyś dwanaście wysp tak czystych, pięknych i bogatych w wodę pitną, że bogowie chcieli utrzymać ich istnienie w tajemnicy przed ludźmi, którzy mogliby je zniszczyć. Za najwspanialsze uważali trzy: Kane-huna-moku, Kahiki i Pali-uli. Zamieszkujący je bogowie postanowili ukryć je przed ludzkim wzrokiem, byli bowiem przekonani, że ich piękno doprowadzi do szaleństwa każdego, kto je ujrzy. Po rozważeniu różnych pomysłów, jak to zrobić – takich jak zabarwienie ich kolorem morza lub przeniesienie na dno oceanu – postanowili, że wyspy będą unosić się w powietrzu.

Od chwili, kiedy wyspy znalazły się na niebie, rozpoczęły swoją nieustającą podróż, przenoszone podmuchami wiatru z miejsca na miejsce. Legenda głosi, że o wschodzie lub zachodzie słońca można czasem dostrzec którąś z nich, unoszącą się daleko na horyzoncie. Kiedy jednak spróbujesz komuś ją wskazać, natychmiast podryfuje dalej lub przyjmie zupełnie inną postać, na przykład pumeksowej tratwy, skalnego odłamka wyrzuconego przy wybuchu wulkanu lub po prostu chmury.

Często przypominałem sobie tę legendę, kiedy prowadziłem swoje śledztwo. Tropione przeze mnie odkrycia bardzo przypominały wspomniane w niej wyspy – egzotyczne obszary, które grupa zadufanych w sobie, samozwańczych władców postanowiła utrzymywać w tajemnicy przed ludzkością. Ja natomiast chciałem się dowiedzieć, jakimi możliwościami inwigilacji dysponuje NSA, czy i na ile ta działalność wykracza poza oficjalny zakres kompetencji, kto to wszystko zatwierdził,

kto o tym wiedział i jak te systemy naprawdę funkcjonowały z technicznego i instytucjonalnego punktu widzenia.

Ilekroć uznałem, że wypatrzyłem jedną z takich „wysp” – napisaną wielkimi literami nazwę kodu, której nie znałem, czy program wspomniany w przypisie ukrytym na końcu raportu – zaczynałem szukać dalszych wzmianek na ten temat w innych dokumentach, ale ich nie znajdowałem. Zupełnie jakby tropiony przeze mnie ślad odpłynął i zniknął. Potem, po kilku dniach lub tygodniach, mógł ponownie się wynurzyć pod innym określeniem w dokumencie z innego działu.

Czasem znajdowałem program o rozpoznawalnej nazwie, ale bez żadnego wyjaśnienia, do czego służy. Innym razem trafiałem na wyjaśnienie bez nazwy i bez wzmianki, czy opisane możliwości dotyczą już działającego projektu, czy są tylko ambitnym planem. Natykałem się na dodatkowe kategorie niejawności w niejawnych dokumentach, zastrzeżenia do zastrzeżeń, pakiety programów w innych pakietach i programy zagnieżdżone w innych programach. To akurat było charakterystyczne dla NSA, gdzie z rozmysłem dbano o to, by lewa ręka nie wiedziała, co czyni prawa.

Kiedyś obejrzałem film dokumentalny o opracowywaniu map, a w szczególności o sporządzaniu ich w czasach, gdy nie było cyfrowych systemów informacji geograficznych – i moje obecne zajęcie w pewnym stopniu mi to przypominało. Dawniej kapitanowie statków prowadzili dzienniki pokładowe i notowali współrzędne, a później kartografowie na lądzie starali się odpowiednio je zinterpretować. Dopiero po setkach lat żmudnego gromadzenia tych danych udało się nam poznać cały obszar Pacyfiku i tamtejsze wyspy.

Ja jednak nie miałem do dyspozycji setek lat ani statków. Byłem sam. Sam, pochylony nad płachtą błękitnego oceanu, starałem się ustalić

położenie plamki suchego lądu, tych znalezionych danych, względem wszystkich innych.

20_Heartbeat|

Kiedy w 2009 roku zastąpiłem jednego z prelegentów podczas brzemiennej w skutki konferencji na temat Chin, chyba zaskarbiłem sobie sympatię kilku osób, przede wszystkim z Międzyagencyjnej Akademii Szkolenia Kontrwywiadowczego (JCITA) i pełniącej nad nią zwierzchnictwo Agencji Wywiadu Departamentu Obrony (DIA). Na przestrzeni następnych trzech lat JCITA zaprosiła mnie na sześć, może siedem konferencji organizowanych na terenie placówek DIA w roli prelegenta lub prowadzącego seminarium. Zostałem w pewnym sensie instruktorem technik, dzięki którym pracownicy amerykańskich służb wywiadowczych mogli zabezpieczać się przed chińskimi hakerami i wykorzystywać informacje pozyskane przez analizę ich cyberataków do odwdzięczania się pięknym za nadobne.

Zawsze lubiłem uczyć – w każdym razie na pewno bardziej niż być uczniem i studentem – a we wczesnej fazie mojego rozczarowania, pod koniec etapu japońskiego i przez okres pracy dla Della, miałem poczucie, że jeśli zdecyduję się pozostać w wywiadzie do końca kariery zawodowej, najłatwiej będzie mi dochować wierności osobistym zasadom i zapewnić umysłowi odpowiedni trening właśnie na stanowiskach akademickich. Prowadzenie zajęć dla JCITA pozostawiało te drzwi otwarte. Dzięki temu mogłem również trzymać rękę na pulsie – jako nauczyciel nie możesz pozwolić sobie na to, by wyprzedzili cię uczniowie, szczególnie jeśli chodzi o technologię.

Nabrałem w związku z tym zwyczaju przeglądania cyfrowych tablic wiadomości, które NSA nazywa readboardami. Pełnią one rolę zbliżoną do blogów poświęconych bieżącym wydarzeniom z tą różnicą, że pojawiające się newsy dotyczą utajnionych działań wywiadowczych. Każda większa placówka NSA prowadzi własną tablicę, gdzie jej personel codziennie zamieszcza najważniejsze i najbardziej interesujące dokumenty z danego dnia – innymi słowy, wszystko, z czym pracownik musi się zaznajomić, by być na bieżąco.

Skutkiem przyzwyczajenia, które pozostało mi po przygotowaniach do wykładów dla JCITA, a także – jeśli mam być szczery – dlatego że nudziłem się na Hawajach, zacząłem codziennie sprawdzać zawartość kilku tablic. Jedna z nich należała do mojej placówki, drugą obsługiwał personel mojego poprzedniego miejsca pracy w Tokio, a kilkoma kolejnymi zarządzano z Fortu Meade. Dzięki temu, jak mało wymagające było moje nowe stanowisko, miałem tyle czasu na czytanie, ile dusza zapragnie. Na wcześniejszym etapie kariery zakres moich zainteresowań mógłby wywołać pewne wątpliwości, ale teraz byłem jedynym pracownikiem Biura Wymiany Informacji – zatem moja praca polegała właśnie na tym, by wiedzieć, jakimi informacjami wartymi wymiany dysponujemy. Tymczasem większość moich kolegów z Tunelu w wolnym czasie oglądała stream Fox News.

W nadziei, że uda mi się uporządkować wszystkie dokumenty, które chciałem przeczytać, napisałem skrypt – tworzył on coś na podobieństwo mojej prywatnej listy „best of” z kilku różnych readboardów. Liczba pobranych plików szybko rosła, aż pewnego dnia sympatyczna pani odpowiedzialna za limity przechowywania wyraziła niezadowolenie z objętości mojego folderu. Zdałem sobie wtedy sprawę, że moja osobista tablica przeistoczyła się z listy aktualności w archiwum poufnych

informacji, którego znaczenie wykraczało daleko poza bieżący dzień. Nie chciałem usuwać plików ani zarzucać aktualizacji, postanowiłem zatem udostępnić innym gromadzoną zawartość. Uznałem to za najlepsze usprawiedliwienie swoich działań, szczególnie że dzięki temu – zasadniczo bez przekraczania upoważnień – zyskałem dostęp do materiałów z szerszego wachlarza źródeł. Za zgodą mojego przełożonego zająłem się zatem budowaniem zautomatyzowanej tablicy wiadomości. Miała aktualizować się sama, a nie polegać na dodawaniu informacji przez personel.

Zaprojektowałem moją platformę podobnie jak EPICSHELTER – by nieustannie skanowała sieć w poszukiwaniu nowych niepowtarzających się dokumentów. Robiła to jednak z dużo większym rozmachem niż mój poprzedni system, sięgała poza NSAnet, czyli sieć NSA, do sieci CIA i FBI, jak również do Międzyagencyjnego Światowego Systemu Łączności Wywiadowczej (JWICS), ściśle tajnego intranetu Departamentu Obrony. Mój plan zakładał, że system będzie udostępniał swoje znaleziska wszystkim agentom NSA na podstawie poziomu poświadczenia bezpieczeństwa zawartego w ich cyfrowym certyfikacie tożsamości, tak zwanym PKI, generując osobistą tablicę wiadomości zgodną z upoważnieniami, zainteresowaniami i przynależnością do określonych jednostek agencji. Zasadniczo miała to być tablica tablic, dopasowany do czytelnika agregator wiadomości dostarczający pracownikom agencji najświeższe informacje związane z ich zadaniami – wszystkie dokumenty, jakie musieli przeczytać, by być na bieżąco. Zamierzałem prowadzić ją z serwera, którego byłem jedynym administratorem, umiejscowionego w pomieszczeniu, do którego wchodziło się z tego samego korytarza, co do mojego miejsca pracy. Serwer ten miał również przechowywać kopie wszystkich pozyskiwanych dokumentów, co umożliwiało mi wykonywanie

głębokich międzyagencyjnych wyszukiwań, o których szefowie większości agencji mogli tylko marzyć.

Nazwałem ten system Heartbeat, ponieważ monitorował bicie serca NSA i innych służb wywiadowczych. Pozyskiwał dokumenty z wewnętrznych stron poświęconych wszelkim specjalnościom, od doniesień o najnowszych projektach badawczych z kryptografii po sprawozdania z zebrań Narodowego Komitetu Obrony. Żyłami Heartbeata płynęła gigantyczna ilość danych. Starannie skonfigurowałem go w taki sposób, by pobierał materiały w równomiernym, nieśpiesznym tempie i nie zawłaszczał sobie podmorskiego kabla światłowodowego spinającego Hawaje z Fortem Meade. Mimo tego ściągał o wiele więcej dokumentów, niż można było robić to manualnie, i w mgnieniu oka stał się najobszerniejszym readboardem w całej sieci NSAnet.

Niedługo po tym, jak serce mojej platformy zaczęło bić, otrzymałem e-mail, który prawie zatrzymał je na zawsze. Administrator z odległej placówki – najwyraźniej jedyny w całym wywiadzie, któremu chciało się przeglądać logi swoich serwerów – zapragnął dowiedzieć się, dlaczego jakiś system z Hawajów kopiuje jak leci rekordy z jego bazy danych. W trosce o bezpieczeństwo natychmiast zablokował mi dostęp i zażądał wyjaśnienia. Napisałem mu, co robię, i pokazałem, w jaki sposób może samodzielnie korzystać ze strony umieszczonej w wewnątrzagencyjnej sieci, żeby czytać wiadomości na Heartbeacie. Jego reakcja przypomniała mi o nietypowej cesze, którą już wcześniej zauważyłem u osób pełniących funkcje techniczne w machinie bezpieczeństwa państwowego: kiedy tylko uzyskał ode mnie dostęp, jego nieufność przeistoczyła się w zainteresowanie. Mógł wątpić w człowieka, ale maszynie ufał w stu procentach. Zobaczył na własne oczy, że Heartbeat zajmuje się wyłącznie tym, do czego został zaprojektowany, i robi to idealnie. Zafascynowało go

moje dzieło. Odblokował mi dostęp do swojego repozytorium danych, a nawet zaproponował, że mi pomoże, rozpowszechniając informację o istnieniu Heartbeata wśród kolegów.

Niemal wszystkie dokumenty, które ujawniłem dziennikarzom, dotarły do mnie za pośrednictwem tego systemu. Dzięki niemu poznałem nie tylko cele aparatu wywiadowczego, ale i zakres jego możliwości w dziedzinie masowej inwigilacji. Chcę jednak wyraźnie podkreślić, że w tym okresie, w połowie 2012 roku, powodowała mną przede wszystkim chęć zrozumienia zasad działania tej formy wywiadu. Tymczasem prawie wszyscy dziennikarze, którzy później podejmowali temat ujawnionych przeze mnie dokumentów, koncentrowali się na osobach szpiegowanych – amerykańskich obywatelach, na przykład, albo głowach sprzymierzonych państw. Innymi słowy, bardziej interesowała ich tematyka przekazów, jakie przechwytywano, niż działanie systemu, który to umożliwiał. Oczywiście rozumiem takie podejście do sprawy, zwłaszcza że sam miałem podobne. Ja jednak przede wszystkim byłem zainteresowany kwestiami natury technicznej. Można się dowiedzieć o założeniach danego programu, czytając jego dokumentację albo wertując slajdy prezentacji w PowerPoincie, ale im lepiej pozna się jego mechanizmy, tym trafniej można ocenić drzemiący potencjał do nadużyć.

Oznaczało to, że nie interesowały mnie zanadto materiały instruktażowe – takie na przykład jak jeden z najszerzej opisywanych plików, które ujawniłem prasie. Chodzi o slajdy z prezentacji powerpointowej z 2011 roku, które przedstawiały nową filozofię wywiadowczą NSA bazującą na sześciu filarach: „Wszystko Wywąchać, Wszystko Poznać, Wszystko Zebrać, Wszystko Przetworzyć, Wszystko Wykorzystać, Wszystko Przekazać”. Był to zwykły piarowy bełkot, marketingowy żargon. Miał zrobić wrażenie na sojusznikach Ameryki:

Australii, Kanadzie, Nowej Zelandii i Anglii – najważniejszych krajach, z którymi Stany Zjednoczone dzielą się informacjami wywiadowczymi. (Razem z USA kraje te tworzą tak zwany Sojusz Pięciorga Oczu). „Wywąchać” oznaczało znaleźć źródło danych. „Poznać” – odkryć, co dane te przedstawiają. „Zebrać” znaczyło je przechwycić. „Wykorzystać” – posłużyć się nimi do realizacji celów agencji. „Przekazać” zaś należało je naszym sojusznikom. Tę taksonomię obejmującą sześć gatunków łatwo było zapamiętać i sprzedać; zresztą trafnie oddawała skalę ambicji NSA oraz zakres tajnych porozumień z rządami innych krajów. Nie dawała mi jednak najmniejszego pojęcia o tym, w jaki sposób dążenia NSA są realizowane od strony technicznej.

Dużo bardziej pouczający był nakaz wystawiony przez Sąd do spraw Wywiadu Zagranicznego (FISA), który znalazłem – prawomocne żądanie, by dana prywatna firma przekazała rządowi federalnemu prywatne dane klientów. Teoretycznie nakazy tego rodzaju wystawiano na mocy prawa powszechnego, ale ich zawartość, a nawet samo istnienie były objęte klauzulą „ściśle tajne”. Zgodnie z paragrafem 215 ustawy antyterrorystycznej Patriot Act, tak zwaną klauzulą o dokumentacji biznesowej, rząd był upoważniony, by zwracać się do sądu FISA o nakazy, które zobowiązywały strony trzecie do udostępnienia „wszelkich istniejących materiałów (…) mających znaczenie” dla wywiadu zagranicznego i dochodzeń w sprawach związanych z terroryzmem. Nakaz sądowy, który zdobyłem, dowodził jednak, że NSA w tajemnicy uznała to upoważnienie za równoznaczne z przyzwoleniem na nieprzerwane gromadzenie wszelakiej „dokumentacji biznesowej” – metadanych – dotyczącej rozmów telefonicznych przepływających przez infrastrukturę amerykańskich telekomów, takich jak Verizon i AT&T. Obejmowało to

oczywiście rejestry rozmów telefonicznych pomiędzy obywatelami amerykańskimi, których zapisywanie jest sprzeczne z konstytucją.

Co więcej, paragraf 702 ustawy regulującej pracę Sądu do spraw Wywiadu Zagranicznego, FISA Amendments Act, pozwala służbom wywiadowczym obierać za cel dowolnego obywatela obcego kraju przebywającego poza granicami Stanów Zjednoczonych, który mógłby przekazywać „informacje o znaczeniu dla wywiadu zagranicznego". Ta szeroka kategoria czyni potencjalnymi celami dziennikarzy, pracowników korporacji, uczelni wyższych i organizacji pomocowych oraz ogromną liczbę innych całkowicie niewinnych osób. NSA uzasadniała tym prawem istnienie dwóch najważniejszych metod inwigilacji internetu: programów PRISM i *upstream collection*.

PRISM umożliwił NSA regularne pobieranie danych gromadzonych przez Microsoft, Yahoo!, Google'a, Facebooka, Paltalka, YouTube'a, Skype'a, AOL i Apple'a, w tym e-maili, zdjęć, rozmów, wideopołączeń, zawartości stron internetowych, historii przeglądania i wszelkich innych informacji zebranych w ich chmurach. Firmy te stały się świadomymi współpracownikami wywiadu. Druga metoda – dla niej NSA stosowało eufemizm *upstream collection* (zbieranie u źródeł) – była pod pewnymi względami jeszcze większym naruszeniem praw obywatelskich. Umożliwiała pobór danych bezpośrednio z elementów architektury internetowej należących do sektora prywatnego – z przełączników i routerów, które kierują ruchem sieciowym na całym świecie, z satelitów krążących po orbitach okołoziemskich i z kabli światłowodowych o wielkiej przepustowości, biegnących dnem oceanów. Gromadzeniem tych informacji zajmowała się jednostka NSA o nazwie Special Sources Operations (Sekcja Źródeł Specjalnych). Produkowała ona tajny sprzęt podsłuchowy i instalowała go na całym świecie w budynkach skorych do

pomocy korporacji dostarczających usługi internetowe. W sumie PRISM (gromadzenie danych z serwerów należących do dostawców telefonii i internetu) oraz bezpośredni monitoring infrastruktury internetowej zapewniły możliwość inwigilacji całej światowej łączności, zarówno bieżącej, jak i zapisanej.

Następny etap mojego dochodzenia miał na celu określenie, w jaki konkretnie sposób NSA gromadziła te dane – innymi słowy, musiałem przeanalizować dokumenty wyjaśniające, które narzędzia współpracują z wyżej wymienionymi programami i na jakiej zasadzie wybierają spośród ogromnej masy hurtowo gromadzonej komunikacji tę wartą większej uwagi. Kłopot polegał na tym, że informacje takie nie pojawiały się w prezentacjach, nawet tych dla osób o najwyższym poświadczeniu bezpieczeństwa. Można było je znaleźć wyłącznie w diagramach inżynieryjnych i na rysunkach technicznych. Zdobycie tych materiałów stało się moim głównym celem. W odróżnieniu od sloganu reklamowego ukutego na potrzeby Pięciorga Oczu stanowiłyby jednoznaczny dowód, że możliwości, o których czytałem, były czymś więcej niż fantazjami menedżera projektu, który przesadził z kofeiną. Nieustannie nagabywano mnie, projektanta systemów, bym budował szybciej i więcej, miałem więc nieprzyjemną świadomość, że agencjom zdarzało się ogłaszać powstanie technologii, zanim stało się to faktem – czasami dlatego, że jakiś nadgorliwy agencyjny promotor obiecał o jedną rzecz za dużo, a czasami z powodu zwykłej, niepohamowanej ambicji.

W tym wypadku technologie umożliwiające pobór danych bezpośrednio z infrastruktury (*upstream collection*) rzeczywiście istniały. Z czasem uzmysłowiłem sobie, że narzędzia te są najbardziej inwazyjnymi spośród wszystkich, które NSA wykorzystuje w swoim systemie masowej inwigilacji, głównie dlatego że działają najbliżej użytkownika – czyli osoby

będącej celem szpiegowania. Wyobraź sobie, że siedzisz przy komputerze i zamierzasz odwiedzić pewną stronę internetową. Otwierasz przeglądarkę, wpisujesz adres i wciskasz enter. Adres URL jest w praktyce żądaniem, które rusza po łączu w poszukiwaniu serwera docelowego. Po drodze jednak, zanim dotrze do tego serwera, musi się przedostać przez TURBULENCE, jedną z najpotężniejszych broni w arsenale NSA.

Ściślej mówiąc, twoje żądanie przechodzi przez kilka tajnych serwerów ustawionych jeden na drugim w wieżę o wysokości mniej więcej regału na książki z czterema półkami. Zestawy takie są zainstalowane zarówno w specjalnych pomieszczeniach największych firm telekomunikacyjnych w krajach sprzymierzonych, jak również w ambasadach USA i amerykańskich bazach wojskowych. Każdy z nich dysponuje dwoma narzędziami pełniącymi krytyczną funkcję. Pierwsze, o nazwie kodowej TURMOIL, zajmuje się „przechwytywaniem biernym”, czyli tworzy kopie przepływających danych. Drugie – TURBINE – zarządza „przechwytywaniem aktywnym”, czyli majstrowaniem przy internetowej aktywności użytkowników.

Możesz wyobrazić sobie, że TURMOIL to strażnik, a jego posterunkiem jest niewidzialna zapora, przez którą musi przedostać się ruch internetowy. Na widok twojego zapytania TURMOIL sięga po jego metadane w poszukiwaniu selektorów, czyli kryteriów, które sygnalizują, że warte jest większej uwagi. Selektorem może być wszystko, co NSA uzna za podejrzane: konkretny adres e-mailowy, numer karty kredytowej albo numer telefonu, lokalizacja geograficzna miejsca pochodzenia oraz celu twoich sygnałów internetowych, a nawet pewne hasła klucze, takie jak „anonimowy serwer proxy” albo „protest”.

Jeśli TURMOIL oznaczy twoją transmisję jako podejrzaną, przekazuje ją TURBINE, a ta przekierowuje ją na serwery NSA. Tam algorytmy

decydują, które z agencyjnych narzędzi – rodzajów złośliwego kodu – zastosować przeciw tobie. Dobór odbywa się zarówno na podstawie strony, jaką próbujesz odwiedzić, jak i oprogramowania zainstalowanego na twoim komputerze oraz jakości połączenia internetowego. Wybrane złośliwe oprogramowanie jest przesyłane z powrotem do systemu TURBINE (przez programy należące do pakietu QUANTUM, jeśli chciałeś zapytać), ten zaś wprowadza je do kanału łącznościowego i dostarcza do ciebie wraz ze stroną, której otwarcia zażądałeś. W rezultacie otrzymujesz całą treść, o jaką ci chodziło, a wraz z nią niezamawiany pakiet wywiadowczy, którego podpięcie zajmuje mniej niż 686 milisekund. I odbywa się w zupełnej tajemnicy przed tobą.

Z chwilą, gdy ten złośliwy kod znajdzie się na twoim komputerze, NSA uzyskuje dostęp nie tylko do twoich metadanych, ale także do zwykłych danych. Staje się właścicielem całego twojego cyfrowego życia.

21_Sygnaliści|

Nie wszyscy pracownicy NSA korzystali z programu SharePoint, którym zarządzałem, ale nawet oni przeważnie znali dostępne w nim kalendarze. Były one w zasadzie takie same jak kalendarze dla grup pozarządowych, tyle że bez porównania droższe. Dla personelu NSA na Hawajach był to podstawowy interfejs do tworzenia harmonogramów z wpisami, gdzie i kiedy należy stawić się na zebranie. Łatwo zgadnąć, że zarządzanie tym niezbyt mnie fascynowało. W ramach urozmaicania sobie tego zadania starałem się, żeby kalendarz zawsze przypominał o wszystkich świętach, i to naprawdę wszystkich – nie tylko państwowych, ale również takich jak Rosz Haszana, Id al-Fitr, Id al-Adha czy Diwali.

Moje ulubione przypadało 17 września. Jest to Constitution Day and Citizenship Day (Dzień Konstytucji i Obywatelstwa), święto ustanowione dla uczczenia wydarzenia z 1787 roku, kiedy to delegaci na Konwencję Konstytucyjną podpisali Konstytucję Stanów Zjednoczonych Ameryki. Dzień ten obchodzi się w całym kraju, ale formalnie rzecz biorąc, nie jest to święto państwowe. Kongres nie uznał dokumentu założycielskiego naszego państwa, a zarazem najstarszej na świecie wciąż stosowanej konstytucji za dostatecznie ważną, żeby przyznać obywatelom płatny dzień wolny od pracy.

Dla służb wywiadowczych Dzień Konstytucji był nieco kłopotliwy, dlatego obchody ograniczały się zazwyczaj do rozesłania przez komórki prasowe bezbarwnego e-maila podpisanego przez wysokiego rangą dyrektora i do ustawienia w najciemniejszym kącie stołówki smutnego

stoliczka upamiętniającego to wydarzenie. Na stoliku leżały bezpłatne egzemplarze konstytucji, wydrukowane, oprawione i podarowane rządowi przez życzliwych i hojnych aktywistów z organizacji takich jak Cato Institute czy Heritage Foundation – bo wywiadowi nie uśmiechało się wydawanie choćby centa z własnych miliardów dolarów na propagowanie swobód obywatelskich za pomocą słowa drukowanego.

Przypuszczam, że pracownicy pojęli, w czym rzecz, skoro przez siedem lat spędzonych w służbach wywiadowczych nigdy nie widziałem, żeby ktoś oprócz mnie brał ze stolika egzemplarz konstytucji. Ponieważ uwielbiam zarówno ironię, jak i – prawie tak samo – upominki reklamowe, zabierałem zawsze kilka. Jeden zostawiałem sobie, a resztę niepostrzeżenie podkładałem kolegom na ich stanowiska pracy. Przez pewien czas miałem zwyczaj opierać swój egzemplarz o kostkę Rubika na biurku i czytać podczas lunchu, starając się, by sos z paskudnej stołówkowej pizzy nie skapnął na słowa „My, naród”*.

Lubiłem czytać konstytucję częściowo dlatego, że jej postanowienia są wspaniałe, po części ze względu na styl jej zapisów, ale głównie z tego powodu, że wkurzało to moich współpracowników. W instytucji, gdzie wszystkie wydrukowane materiały muszą trafić do niszczarki, gdy tylko przestają być potrzebne, każdy zwraca uwagę na obecność książki na biurku. Zaciekawieni koledzy nie mogli się oprzeć, żeby nie podejść i nie spytać:

– Co tam masz?

– Konstytucję.

Słysząc to, robili dziwne miny i powoli się wycofywali.

W Dzień Konstytucji w 2012 roku jak zwykle zabrałem egzemplarz ze stolika, ale tym razem nie dla żartu. Uświadomiłem sobie, że już od kilku lat nie zapoznałem się z konstytucją w całości (chociaż z zadowoleniem

zauważyłem, że nadal potrafię wyrecytować z pamięci preambułę). Tym razem przeczytałem wszystko: od pierwszych artykułów po ostatnie poprawki. Ta lektura przypomniała mi, co mnie ponownie zaskoczyło – że połowa Karty Praw Stanów Zjednoczonych, czyli pierwszych dziesięciu poprawek, miała na celu utrudnienie pracy organom ochrony porządku publicznego. Szczególnie starannie sformułowano poprawki czwartą, piątą, szóstą, siódmą i ósmą – by poskromić organy rządowe, kreując pewną niewydolność rządzących i ograniczając w ten sposób nadużywanie władzy i prowadzenie inwigilacji.

Najwyraźniej widać to w treści czwartej poprawki, która miała chronić obywateli i ich własność przed kontrolą państwową: „Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać przez bezzasadne rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone”.

Jak należy to rozumieć? Jeśli stróże prawa chcą grzebać w twoim życiu, muszą najpierw udać się do sędziego i pod przysięgą przedstawić prawdopodobny powód usprawiedliwiający takie działanie. Muszą wyjaśnić sędziemu, jakie mają przesłanki, by sądzić, że mogłeś popełnić konkretne przestępstwo lub że określone dowody konkretnego przestępstwa mogą się znajdować w twoim posiadaniu lub w konkretnej części twojej własności. Potem muszą przysiąc, że podają ten powód uczciwie i w dobrej wierze. Tylko wówczas, gdy sędzia wyda nakaz, będzie im wolno rozpocząć przeszukanie i prowadzić je wyłącznie przez ograniczony czas.

Konstytucję spisano w XVIII wieku, kiedy do obliczeń zamiast komputerów używano abakusów, liczydeł lub sumatorów, a przesyłanie

informacji za pomocą statków trwało tygodniami lub miesiącami. Wydaje się oczywiste, że pliki komputerowe, niezależnie od zawartości, stanowią współczesną wersję wspomnianych w konstytucji „dokumentów". Niewątpliwie korzystamy z nich tak, jak korzysta się z dokumentów, szczególnie z plików tekstowych, arkuszy obliczeniowych, wiadomości i historii przeglądarek. Dane to z kolei nasze „mienie" – bardzo pojemne określenie wszystkiego, co posiadamy, wytwarzamy, sprzedajemy i kupujemy online. Domyślnie obejmuje ono również metadane – informacje opisujące to wszystko i stanowiące dokładny zapis naszego prywatnego życia.

Kilkaset lat po podpisaniu konstytucji komputery, chmury i telefony stały się naszymi domami, równie osobistymi i prywatnymi jak fizyczne budynki i mieszkania. Jeśli się z tym nie zgadzasz, odpowiedz sobie uczciwie na następujące pytanie: czy wolałbyś pozwolić współpracownikom, żeby przez godzinę swobodnie i samotnie chodzili po twoim domu, czy żeby spędzili choćby dziesięć minut sam na sam z twoim odblokowanym telefonem?

Programy inwigilacyjne NSA, szczególnie krajowe, realizowano z całkowitym brakiem poszanowania dla czwartej poprawki. Agencja zasadniczo twierdziła, że we współczesnym życiu gwarantowana przez ten zapis ochrona nie ma zastosowania. W swojej polityce wewnętrznej NSA nie uznawała danych osobistych za twoją prawnie chronioną własność osobistą ani gromadzenia przez siebie tych danych za „rewizję" lub „zatrzymanie". Stała za to na stanowisku, że skoro już „udostępniłeś" rejestry połączeń telefonicznych „stronie trzeciej", czyli swojemu operatorowi telekomunikacyjnemu, to tym samym straciłeś przysługujące ci konstytucyjnie prawo do prywatności. Ponadto utrzymywała, że do

„rewizji” lub „zatrzymania” dochodzi tylko wówczas, gdy analitycy, a nie algorytmy, aktywnie badają to, co zostało już automatycznie zgromadzone.

W praktyce zatem wywiad twierdził, że sam akt korzystania z nowoczesnych technologii jest równoznaczny z rezygnacją z prawa do prywatności. Gdyby konstytucyjne mechanizmy nadzoru działały prawidłowo, taka skrajna interpretacja czwartej poprawki zostałaby odrzucona przez Kongres i sądy. Ojcowie założyciele Stanów Zjednoczonych byli wytrawnymi graczami w dziedzinie podziału władzy politycznej, szczególnie wyczulonymi na zagrożenia związane z wybiegami prawnymi i prezydenckimi ciągotami do sprawowania autokracji. Zabezpieczeniem przed tym miał być stworzony przez nich ustrój polityczny oparty na podziale władzy pomiędzy trzy równorzędne podmioty, zdefiniowane w trzech pierwszych artykułach konstytucji, co gwarantowało działanie mechanizmów kontroli i równowagi. Okazało się jednak, że gdy przyszło do ochrony prywatności amerykańskich obywateli w erze cyfrowej, każdy z tych podmiotów zawiódł na swój sposób tak, że cały system zawiesił się i stanął w ogniu.

Władza wykonawcza, czyli Kongres składający się z Senatu i Izby Reprezentantów, chętnie zrzekła się funkcji nadzorczej. Mimo że liczba pracowników sił wywiadowczych i współpracujących prywatnych wykonawców gwałtownie rosła, grono Kongresu informowane o kompetencjach i działaniach wywiadu nieustannie malało, aż skurczyło się do kilku członków specjalnych komisji dowiadujących się o operacjach agencji na posiedzeniach za zamkniętymi drzwiami. I nawet oni otrzymywali tylko okrojone informacje. Kiedy już dochodziło do rzadkich publicznych przesłuchań przez Kongres, NSA bez ogródek przedstawiała swoje stanowisko. Agencja nie będzie współpracować, nie będzie udzielać odpowiedzi zgodnych z prawdą i co gorsza, powołując się na konieczność

utajniania różnych faktów, zmusi amerykańskie organy ustawodawcze do współpracy przy zwodzeniu społeczeństwa. Przykładowo, na początku 2013 roku James Clapper, ówczesny dyrektor Wywiadu Narodowego, zeznał pod przysięgą przed Komisją do spraw Wywiadu Senatu Stanów Zjednoczonych, że NSA nie zajmuje się masowym gromadzeniem danych z komunikacji obywateli amerykańskich. Na pytanie: „Czy NSA gromadzi jakikolwiek typ danych dotyczących milionów lub setek milionów Amerykanów?" Clapper odparł, że nie, po czym dodał: „Mogą zdarzać się przypadki nieumyślnego gromadzenia, ale nie celowo". Było to oczywiście świadome bezczelne kłamstwo, wypowiedziane nie tylko przed Kongresem, ale i przed narodem amerykańskim. Wielu kongresmenów, przed którymi zeznawał Clapper, dobrze wiedziało, że dyrektor mija się z prawdą, ale nie zdecydowali się lub nie mieli możliwości prawnych, by zakwestionować jego słowa.

Porażka systemu sądowniczego była jeszcze bardziej rozczarowująca. Sąd do spraw Wywiadu Zagranicznego (FISC), nadzorujący inwigilację przez inne kraje na terenie Stanów Zjednoczonych, jest specjalistycznym organem odbywającym tajne posiedzenia i przesłuchującym tylko organy ścigania i rządowe agencje wywiadowcze. Utworzono go, by wydawał indywidualne nakazy i zezwolenia na gromadzenie danych dotyczących obcego wywiadu. FISC zawsze przychylnie traktował NSA, co wyrażało się w akceptowaniu ponad 99 procent wniosków tej agencji. Tak wysoki odsetek sprawia, że działanie sądu kojarzy się bardziej z przybijaniem pieczątki niż z rozstrzyganiem spraw podczas starannie przeprowadzonych procesów. Po 11 września sąd otrzymał poszerzone kompetencje. Dotychczas zatwierdzał obserwację poszczególnych osób, na przykład zagranicznego terrorysty nr 1 lub zagranicznego szpiega nr 2. Natomiast od tej przełomowej daty zaczął wydawać orzeczenia o legalności i zgodności

z konstytucją szeroko zakrojonych programów inwigilacyjnych, takich jak PRISM i bezpośredni pobór danych z infrastruktury (*upstream collection*), które praktycznie nie podlegały żadnej kontroli. Analiza struktury tych działań przez sąd ograniczała się – zdaniem American Civil Liberties Union (ACLU, Amerykańskiego Związku Swobód Obywatelskich) – do niejawnego legalizowania przez sąd tajnych programów w wyniku utajnionych reinterpretacji prawa federalnego.

Kiedy organizacje ochrony praw obywatelskich, takie jak ACLU, próbowały przeciwstawić się działaniom NSA w normalnych sądach na jawnych posiedzeniach, dochodziło do czegoś dziwnego. Organizacja rządowa wcale się nie broniła i nie wykazywała legalności i konstytucyjności swoich działań. Zamiast tego dowodziła, że ACLU i jej klienci nie mają prawa składać pozwu, bowiem nie posiadają dowodów na jakąkolwiek inwigilację. Ponadto ACLU nie może wykorzystać postępowania sądowego do szukania dowodów na inwigilację, bo istnienie (lub nieistnienie) tych dowodów jest tajemnicą państwową, a przecieki do prasy nie mają znaczenia. Innymi słowy, sąd nie mógł uznać za dowód informacji upublicznionych przez media, a tylko te, których upublicznienie oficjalnie potwierdziły instytucje rządowe. Powołanie się na tajność informacji oznaczało, że ani ACLU, ani nikt inny nie zdoła znaleźć podstaw prawnych do złożenia pozwu, który byłby rozpatrzony na posiedzeniu jawnym w zwykłym sądzie. Ku mojemu oburzeniu w lutym 2013 roku Sąd Najwyższy Stanów Zjednoczonych stosunkiem głosów pięć do czterech zgodził się z uzasadnieniem rządu i oddalił powództwa ACLU i Amnesty International podważające legalność masowej inwigilacji, nawet nie rozważając, czy działania NSA są zgodne z prawem.

Wreszcie jest władza wykonawcza, pierwszy winowajca, jeśli chodzi o naruszanie zapisów konstytucji. Gabinet prezydenta za pośrednictwem

Departamentu Sprawiedliwości popełnił grzech pierworodny polegający na wydaniu tajnego rozporządzenia wykonawczego, które zezwalało na masową inwigilację, co było następstwem wydarzeń z 11 września. W późniejszych latach władza wykonawcza wielokrotnie posuwała się za daleko, a kierownictwa obu partii starały się grać do jednej bramki i ustalać posunięcia obchodzące prawo. Posunięcia, których nikt nie mógł kwestionować, bo klauzula tajności nie dopuszczała ich upubliczniania.

System konstytucyjny tylko wówczas spełnia swoje zadanie, kiedy każda władza z zapisanego w niej trójpodziału funkcjonuje tak, jak powinna. Natomiast kiedy wszystkie trzy nie tylko zawodzą, ale robią to celowo i w skoordynowany sposób, w rezultacie powstaje kultura bezkarności. Zdałem sobie sprawę, że naiwnością było oczekiwać, że Sąd Najwyższy, Kongres lub prezydent Obama, starający się zdystansować od rządów George'a W. Busha, kiedykolwiek pociągną służby wywiadowcze do odpowiedzialności za cokolwiek. Nadeszła pora pogodzić się z tym, że wywiad uważa za uzasadnione swoje działania ponad prawem – i co gorsza, biorąc pod uwagę nieskuteczność organów sądowniczych, ma rację. Przedstawiciele wywiadu zrozumieli zasady rządzące naszym systemem lepiej od jego twórców i obrócili je na własną korzyść.

Zhakowali Konstytucję.

Stany Zjednoczone zrodziły się z aktu zdrady stanu. Deklaracja Niepodległości była bulwersującym naruszeniem praw Anglii, ale przy tym również najpełniejszym wyrażeniem praw natury, na których się opierała, a które zakładały między innymi prawo do przeciwstawienia się władzy oraz buntu w imię zasad podyktowanych człowiekowi przez sumienie. Pierwsi Amerykanie – pierwsi demaskatorzy czy też sygnaliści

w amerykańskiej historii – skorzystali z tego prawa rok później, w 1777 roku.

Mężczyźni ci, podobnie jak wielu w mojej rodzinie, byli marynarzami, oficerami Marynarki Kontynentalnej, i wypłynęli w morze, by bronić swojej nowej ojczyzny. Podczas rewolucji amerykańskiej służyli na uzbrojonej w trzydzieści dwa działa fregacie USS Warren pod dowództwem komodora Eseka Hopkinsa, będącego również głównym dowódcą marynarki. Hopkins był człowiekiem o trudnym, nieustępliwym charakterze i nie miał najmniejszej ochoty angażować swojego okrętu w walkę. Jego oficerowie twierdzili też, że widzieli, jak bił i głodził brytyjskich jeńców wojennych. Dziesięciu oficerów z Warrena postanowiło posłuchać sumienia i kładąc na szali własną karierę, zwróciło się wyżej z relacją o sytuacji na okręcie Komisji Morskiej w podpisanym przez nich wszystkich piśmie:

> Wielce Szanowni Panowie,
>
> my, którzy przedstawiamy tę prośbę, zaciągnęliśmy się na okręt Warren kierowani najszczerszym pragnieniem i niezmiennym oczekiwaniem, że będziemy mogli służyć swojemu krajowi. Nadal niepokoimy się o dobro Ameryki i niczego nie pragniemy goręcej, niż zobaczyć, jak zapanuje w kraju pokój i dobrobyt. Jesteśmy gotowi zaryzykować wszystkim, co nam drogie, i jeśli to będzie konieczne, poświęcić własne życie dla dobra naszej ojczyzny. Pragniemy brać aktywny udział w obronie konstytucyjnych swobód i przywilejów przed prześladowaniami oraz niesprawiedliwymi i okrutnymi roszczeniami tyranii. Przy tym jednak, jak wygląda obecnie sytuacja na pokładzie fregaty, sądzimy, że nie ma perspektyw, byśmy mogli być użyteczni na swoim obecnym posterunku. Znajdujemy się w tej sytuacji już od długiego czasu. Osobiście dobrze poznaliśmy prawdziwy charakter i postępowanie naszego dowódcy, komodora Hopkinsa, i korzystamy z tego sposobu, bo nie mamy bardziej odpowiedniej okazji, żeby szczerze i pokornie zwrócić się do czcigodnej

> Komisji Morskiej z prośbą o zbadanie jego postawy i zachowania, bo przypuszczamy, że ma taki charakter i dopuścił się takich przestępstw, iż nie jest odpowiednią osobą na publiczne stanowisko, które obecnie zajmuje, a o rzeczonych przestępstwach my, sygnatariusze, możemy w należytym stopniu zaświadczyć.

Po otrzymaniu listu Komisja Morska zbadała sprawę i przesłuchała komodora Hopkinsa. Ten w odwecie zwolnił oficerów i resztę załogi, po czym w napadzie gniewu złożył doniesienie na midszypmena Samuela Shawa i trzeciego oficera Richarda Marvena, dwóch podwładnych, którzy przyznali się do napisania petycji, domagał się też postawienia im zarzutów karnych zniesławienia. Sprawa miała być rozpatrywana w sądzie Rhode Island, gdzie ostatnim kolonialnym gubernatorem był Stephen Hopkins, sygnatariusz Deklaracji Niepodległości i brat komodora.

Do prowadzenia procesu wyznaczono sędziego wskazanego przez gubernatora Hopkinsa. Shawa i Marvena uratował inny oficer marynarki, John Grannis, ponieważ przedstawił sprawę bezpośrednio przed Kongresem Kontynentalnym. Przekonał członków Kongresu, których dodatkowo zaniepokoiła możliwość stworzenia precedensu – postawienie karnego zarzutu zniesławienia wojskowym, którzy donieśli o zaniedbaniu obowiązków przez przełożonego. W rezultacie 30 lipca 1778 roku Kongres usunął komodora Hopkinsa ze stanowiska dowódcy, nakazał Skarbowi pokrycie kosztów prawników Shawa i Marvena oraz jednogłośnie przyjął pierwszą amerykańską ustawę chroniącą sygnalistów. Ustawa głosiła, że „obowiązkiem wszystkich osób będących w służbie Stanów Zjednoczonych oraz wszystkich innych mieszkających w tym państwie, którzy dowiedzą się o niewłaściwym postępowaniu, oszustwach i występkach funkcjonariuszy publicznych lub osób pozostających w służbie tych stanów,

jest jak najwcześniejsze poinformowanie o nich Kongresu lub innych odpowiednich organów”.

To prawo dało mi nadzieję – i nadal daje. Nawet w najtrudniejszych chwilach wojny o niepodległość, kiedy ważyło się istnienie mojego kraju, Kongres nie tylko zezwolił na akty buntu wynikające z wierności zasadom, ale wręcz nadał im rangę obowiązku. I właśnie z tego obowiązku postanowiłem się wywiązać; taką decyzję podjąłem w drugiej połowie 2012 roku. Oczywiście wiedziałem, że będę ujawniał informacje w zupełnie innych czasach, z jednej strony łatwiejszych, a z drugiej bardziej przepełnionych cynizmem. Niewielu, a być może żaden z moich przełożonych nie poświęciłby kariery dla tych samych amerykańskich zasad, dla których nasi żołnierze często oddają życie. Nie mogłem jak dziesięciu marynarzy z Warrena udać się do osób postawionych wyżej w hierarchii, co służby wywiadowcze nazywają skorzystaniem z właściwych kanałów. Nie wchodziło to w grę z prostego powodu: moi przełożeni nie tylko doskonale wiedzieli, co robi agencja, ale sami tym wszystkim kierowali – byli współwinni.

W organizacjach takich jak NSA – gdzie bezprawne postępowanie tak wrosło w funkcjonowanie instytucji, że nie wynika z indywidualnej inicjatywy, lecz staje się ideologią – „właściwe kanały” pełnią bowiem funkcję pułapki wyłapującej heretyków i niezadowolonych. Miałem już okazję przekonać się o zawodności hierarchii służbowej w Warrenton i potem w Genewie, gdzie wykonując swoje obowiązki, wykryłem luki w zabezpieczeniach niezwykle ważnego programu. Zgłosiłem to wyżej, a kiedy nic nie zrobiono w tej sprawie, poinformowałem również o tej bierności. Moi przełożeni byli z tego niezadowoleni, bo z kolei ich przełożeni też nie byli tym zachwyceni. Łańcuch zarządzania jest

prawdziwym łańcuchem: krępuje wszelkie poczynania, a niższe jego ogniwa mogą zostać poruszone tylko w wyniku działania tych wyższych.

Pochodzę z rodziny, której członkowie służyli w Straży Wybrzeża, toteż zawsze mnie fascynowało, jak wiele angielskich słów związanych z ujawnianiem informacji ma podtekst morski. Nawet przed czasami okrętu USS Warren w różnych organizacjach – zupełnie jak na statkach – dochodziło do „przecieków". Kiedy statki zamiast wiatru zaczęły używać do napędu pary, korzystano z gwizdków sygnalizujących zamiary i zagrożenia – jeden gwizdek przy mijaniu się lewą burtą, dwa przy mijaniu się prawą, pięć jako ostrzeżenie; stąd właśnie zaczerpnięto określenie *whistleblower* (dmuchający w gwizdek) oznaczające sygnalistę.

Nazwy demaskatorów w wielu innych europejskich językach ulegały zmianom, gdy wydarzenia historyczne zmieniały ich wydźwięk. We Francji długo posługiwano się określeniem *dénonciateur*, ale kiedy podczas drugiej wojny światowej nabrało skojarzeń z denuncjatorem donoszącym na rodaków Niemcom, zaczęto preferować określenie *lanceur d'alerte* (osoba ostrzegająca). Z kolei w Niemczech borykających się ze spuścizną nazistów i Stasi zrezygnowano ze słów *Denunziant* i *Informant*, decydując się na nie do końca zadowalające *Hinweisgeber* (dostarczający wskazówek), *Enthueller* (ujawniający), *Skandalaufdecker* (odkrywający skandale), a nawet zabarwione politycznie *ethische Dissidenten* (dysydent moralny). Tymczasem w języku niemieckim online rzadko korzysta się z tych wszystkich określeń, bowiem w odniesieniu do współczesnego, zazwyczaj opartego na internecie ujawniania informacji używa się angielskiego rzeczownika *whistleblower* i czasownika *leaken*. Natomiast w reżimach takich jak w Rosji i Chinach demaskatorów nazywa się słowami zabarwionymi pejoratywnie, jak na przykład „donosiciel" czy „zdrajca". W takich społeczeństwach musiałaby przez dłuższy czas istnieć silna wolna

prasa, żeby nadać używanym tam określeniom bardziej pozytywne zabarwienie albo stworzyć nowe terminy, które oddawałyby fakt, że demaskatorstwo to nie zdrada, lecz honorowy obowiązek.

Ostatecznie każdy język, także angielski, manifestuje stosunek danej kultury do władzy tym, jak definiuje akt ujawnienia informacji. I nawet wywodzącymi się z dziedziny marynarki angielskimi określeniami, pozornie neutralnymi i łagodnymi, czyn ten przedstawia się z punktu widzenia instytucji, która uważa się za skrzywdzoną, a nie społeczeństwa, które ta organizacja zawiodła. Kiedy instytucja potępia przeciek, sugeruje, że jego sprawca coś uszkodził lub zniszczył.

Obecnie wyrazy „przeciek” i „demaskatorstwo” traktuje się często wymiennie. Moim zdaniem termin „przeciek” należy stosować inaczej, niż się to na ogół robi. Określenie to powinno być używane w odniesieniu do aktów ujawnienia informacji dokonywanych nie w publicznym, lecz we własnym interesie lub dla osiągnięcia określonych celów instytucjonalnych czy politycznych. Mówiąc ściślej, przeciek w moim rozumieniu polega na podłożeniu dowodów lub sianiu propagandy. Jest to wybiórcze ujawnienie tajnych informacji w celu zachwiania powszechnym przekonaniem lub wpłynięcia na określone decyzje. Praktycznie nie ma dnia, żeby jakiś „anonimowy”, wysoki rangą urzędnik państwowy nie napomknął dziennikarzowi o poufnej sprawie, której wypłynięcie pomaga zrealizować plany jego instytucji lub partii.

Chyba najdobitniejszym przykładem takiej polityki jest sytuacja z 2013 roku, kiedy wyżsi urzędnicy Wspólnoty Wywiadów prawdopodobnie postanowili rozdmuchać zagrożenie terroryzmem lub wyciszyć krytykę masowej inwigilacji i wysłali do kilku portali informacyjnych niezwykle szczegółowe raporty z podsłuchu rozmowy konferencyjnej, jaką Ajman al-Zawahiri, przywódca Al-Kaidy, przeprowadził z członkami tej organizacji

z całego świata. Podczas tej tak zwanej rozmowy konferencyjnej Legionu Zagłady al-Zawahiri rzekomo omawiał współpracę organizacyjną z Nasserem al-Wuhayshim, przywódcą Al-Kaidy w Jemenie, oraz przedstawicielami Talibów i Boko Haram. Ujawniając swoją zdolność do przechwycenia tej rozmowy – o ile wierzymy w ten przeciek, który nie był nagraniem, tylko zapisem – służby wywiadowcze nieodwracalnie poświęciły doskonałe możliwości poznawania planów i zamiarów najwyższych rangą przywódców terrorystów wyłącznie dla doraźnych politycznych korzyści. Co więcej, za ów przeciek nikogo nie pociągnięto do odpowiedzialności, choć z pewnością był niezgodny z prawem i pozbawił USA możliwości dalszych podsłuchów takiego doskonałego źródła informacji o Al-Kaidzie.

Amerykańska klasa polityczna raz za razem udowadnia, że gotowa jest tolerować przecieki, a nawet do nich doprowadzać, jeśli tylko służy to jej interesom. Wywiad często chwali się „sukcesami", nawet jeśli dotyczą spraw utajnionych, których ujawnienie ma poważne konsekwencje. W ostatnich czasach absurdalność tego postępowania była najbardziej widoczna w przeciekach dotyczących pozasądowej egzekucji w Jemenie Anwara al-Awlakiego, urodzonego w USA radykalnego duchownego. Administracja Obamy, która na łamach „Washington Posta" i „New York Timesa" upubliczniła wykorzystanie drona do zabójstwa al-Awlakiego, tym samym milcząco potwierdziła wykorzystywanie samolotów bezzałogowych w działaniach CIA oraz istnienie tzw. *disposition matrix*, czyli listy osób do usunięcia, przy czym jedno i drugie jest oficjalnie ściśle tajne. W ten sposób przyznano również, że Stany Zjednoczone nie tylko stosują praktyki selektywnej eliminacji w ogóle, ale robią to również w stosunku do obywateli amerykańskich. Te skoordynowane przecieki ujawniające informacje w postaci kampanii medialnej były wstrząsającym dowodem na

dwulicowe podejście administracji rządowej do tajności: z jednej strony należy jej przestrzegać, żeby rząd mógł bezkarnie działać, ale z drugiej zapomina się o niej, kiedy rządzący chcą przypisać sobie zasługi.

I dopiero w tym kontekście można w pełni zrozumieć taką zmienność w rozumieniu przecieków. Rząd USA wybacza „nieautoryzowane" przecieki, kiedy przynoszą nieoczekiwane korzyści, i zapomina o „autoryzowanych", gdy wyrządzają szkody. Ale skoro szkodliwość i brak zezwolenia, nie wspominając już o nielegalności, mają niewielki wpływ na reakcję rządu, to co ma? Co sprawia, że niektóre informacje można ujawniać, a innych nie?

Odpowiedź brzmi: władza i kontrola. Przeciek może być zaakceptowany, jeśli nie podważa głównych prerogatyw danej instytucji. Gdyby wszystkie szczeble organizacji, od kancelarii pocztowej po naczelne kierownictwo, miały takie same uprawnienia do omawiania spraw wewnętrznych, kadra kierownicza musiałaby zrzec się swojej kontroli nad informacjami i dalsze działanie instytucji byłoby zagrożone. Przyznanie sobie tej równości głosu, niezależnie od pozycji w hierarchii firmy, i korzystanie z niej jest właśnie demaskatorstwem. Takie postępowanie jest szczególnie groźne dla wywiadu, który działa w oparciu o ścisłe rozgraniczenie poszczególnych komórek za prawną zasłoną tajności.

Sygnalista to według mojej definicji osoba, która po trudnych doświadczeniach doszła do wniosku, że jej działalność w danej organizacji stała się niezgodna z zasadami obowiązującymi w społeczeństwie poza obrębem tejże – i nielojalna wobec ogółu – choć instytucja ta powinna przed społeczeństwem odpowiadać. Ta osoba wie, że nie może dłużej pozostać w organizacji oraz że organizacja nie zostanie rozwiązana. Sądzi jednak, że być może uda się ją zreformować i dlatego demaskuje

nieprawidłowości, ujawniając tajne informacje, co ma doprowadzić do wywarcia na instytucję presji społecznej.

Jest to trafny opis sytuacji, w której się znalazłem, choć winny jestem ważne uzupełnienie, a mianowicie wszystkie informacje, które zamierzałem ujawnić, były sklasyfikowane jako ściśle tajne. Ponadto nie wystarczyłoby upublicznienie samych tajnych programów. Musiałem zdemaskować cały system poufności informacji i wykazać, że nie jest to – jak twierdziły służby wywiadowcze – absolutna prerogatywa państwa, tylko przywilej nadużywany przez wywiad w celu uniknięcia demokratycznego nadzoru. Bez pokazania całego zakresu tej systemowej tajności nie byłoby mowy o przywróceniu równowagi sił pomiędzy obywatelami a rządem. I właśnie chęć przywrócenia prawidłowej sytuacji jest dla mnie kluczowa dla demaskatorstwa. Dlatego nie mamy tu do czynienia z radykalnym aktem niezgody czy oporu, lecz ze zwykłym powrotem – daniem sygnału statkowi, że musi wrócić do portu, gdzie zostanie częściowo rozebrany i wyposażony na nowo, a przyczyny przecieków – usunięte. I dopiero wówczas będzie mógł znowu ruszyć w drogę.

Jedyną reakcją współmierną do skali przestępstwa było dla mnie całkowite odsłonięcie całego aparatu masowej inwigilacji, i to nie przeze mnie, tylko przez media – w istocie czwartą władzę naszego państwa, chronioną Kartą Praw Stanów Zjednoczonych. Z pewnością nie wystarczyłoby ujawnienie jednego uchybienia lub nawet kilku nadużyć, bo agencja zaprzestałaby tych działań (lub przynajmniej stwarzałaby takie pozory), a jednocześnie cała reszta systemu pozostałaby nietknięta. Dlatego byłem zdecydowany wyciągnąć na światło dzienne jeden fakt o całokształcie działalności wywiadu: mój rząd opracował i wdrożył globalny system masowej inwigilacji bez wiedzy i zgody obywateli.

W odpowiednich okolicznościach sygnalistą może zostać osoba dowolnego szczebla hierarchii. Dzięki technologii informatycznej nastały jednak czasy, kiedy po raz pierwszy w znanej nam historii najskuteczniejsi mogą być pracownicy piastujący stanowiska na niższych szczeblach drabiny, którym najmniej zależy na utrzymaniu istniejącego stanu rzeczy. W służbach wywiadowczych, podobnie jak praktycznie we wszystkich przerośniętych i zdecentralizowanych instytucjach, gdzie praca opiera się na komputerach, te niższe posady pełne są pracowników technicznych, takich jak ja, których uprawniony dostęp do najważniejszej infrastruktury jest zupełnie nieproporcjonalny do oficjalnych możliwości wpływania na decyzje organizacji. Innymi słowy: zwykle występuje zdecydowany brak równowagi pomiędzy tym, co osoby takie jak ja – zdaniem kierownictwa – powinny wiedzieć, a tym, czego potrafimy się dowiedzieć; pomiędzy naszymi niewielkimi możliwościami zmiany kultury instytucji a ogromnymi możliwościami przedstawienia ogółowi społeczeństwa tego, co nas niepokoi. Niewątpliwie mogą się zdarzać akty nadużycia takich technologicznych przywilejów – w końcu większość pracowników technicznych odpowiedzialnych za działanie systemu ma dostęp do wszystkiego – ale prerogatywy te najczęściej wykorzystuje się w przypadkach dotyczących samej technologii. Specjalistyczne umiejętności pociągają za sobą większą odpowiedzialność. Specjaliści, którzy chcą ujawnić niewłaściwe wykorzystanie technologii, nie mogą tylko po prostu poinformować o tym opinię publiczną. Jeśli znaczenie ich odkryć ma być dobrze zrozumiane, mają obowiązek wyjaśnić i przedstawić sprawę w odpowiednim kontekście.

Kilkadziesiąt osób z całego świata, które najbardziej nadawały się do tego, by podjąć takie kroki, znajdowało się właśnie tutaj – siedziały niedaleko mnie w Tunelu. Moi koledzy i koleżanki pracujący tu na

stanowiskach technicznych przychodzili codziennie, zajmowali miejsca przy terminalach i wykonywali zadania dla kraju. Nie byli zwyczajnie nieświadomi dokonywanych przez władze nadużyć. Nie. Ich to po prostu nie interesowało. Ten brak ciekawości sprawiał, że nie wydawali mi się postaciami złymi, lecz tragicznymi. Nie miało znaczenia, czy zaczęli pracować w wywiadzie z pobudek patriotycznych, czy oportunistycznych; kiedy już dostali się do tej machiny, sami stali się maszynami.

---

* Źródło wszystkich cytatów z Konstytucji Stanów Zjednoczonych: *Konstytucja Stanów Zjednoczonych Ameryki*, przeł. Andrzej Pułło, Wydawnictwo Sejmowe, Warszawa 2002, http://libr.sejm.gov.pl/tek01/txt/konst/usa.html [dostęp 6.08.2019] (przyp. tłum.).

22_Czwarta_władza|

Nie ma nic trudniejszego niż być obarczonym sekretem, którym nie możesz podzielić się z innymi. Jeśli twoja praca wymaga posługiwania się fałszywą tożsamością albo ukrywania faktu, że pracujesz w podziemnym biurze, położonym pod najpilniej strzeżoną plantacją ananasów na świecie, obowiązek zachowania milczenia może ci ciążyć, ale przynajmniej masz świadomość, że jesteś częścią zespołu. Wasze obowiązki objęte są tajemnicą, ale jest to wspólna tajemnica i wspólnie dźwigacie jej ciężar. Takie życie bywa trudne, ale jest w nim miejsce także na śmiech.

Ale kiedy skrywasz sekret, którego nie możesz ujawnić absolutnie nikomu, nawet śmiech zaczyna brzmieć fałszywie. Mogłem mówić o tym, co mnie niepokoiło, ale nie wolno mi było wspomnieć o wnioskach, do jakich prowadziły mnie moje obawy. Kiedy próbowałem tłumaczyć kolegom z pracy, że to, co robimy, niszczy wartości, których przysięgaliśmy chronić, za każdym razem słyszałem to samo: „Nic na to nie poradzisz”. Nienawidziłem tego stwierdzenia wraz z pobrzmiewającym w nim poczuciem rezygnacji i niemocy. Zarazem jednak słowa moich kolegów skłoniły mnie do zadania sobie pytania: „Czy naprawdę nie mogę nic na to poradzić?”.

Odpowiedź przyszła sama. Postanowiłem podjąć się roli demaskatora. Zdawałem sobie sprawę, że jeśli wspomnę o tej decyzji Lindsay, miłości mojego życia, to wystawię nasz związek na ciężką próbę – znacznie cięższą, niż gdybym zachował przed nią tajemnicę. Nie chcąc przysparzać

jej niepotrzebnego cierpienia, zdecydowałem się milczeć i tym samym skazałem się na milczenie w samotności.

Sądziłem, że łatwo będzie mi znieść osamotnienie i izolację, a w każdym razie spodziewałem się, że zniosę je lepiej niż inni demaskatorzy. Czy moje dotychczasowe życie nie przygotowało mnie do wyzwania, jakie zamierzałem teraz podjąć? Czy przez te wszystkie lata, spędzone w niemym zachwycie przed ekranem komputera, nie przywykłem wystarczająco do samotności? Byłem działającym w pojedynkę hakerem, kapitanem portu na nocnej zmianie, strażnikiem kluczy w opustoszałym nocą biurze. Sęk w tym, że byłem również człowiekiem i doskwierał mi brak kogoś, z kim mógłbym dzielić moje brzemię. Każdego dnia toczyłem wewnętrzne zmagania, bez powodzenia usiłując pogodzić nakazy prawa z głosem sumienia, obowiązki z pragnieniami. Miałem wszystko, na czym mi zależało, czyli miłość i rodzinę, a do tego odniosłem sukces wykraczający poza moje najśmielsze oczekiwania; można powiedzieć, że żyłem w raju i mogłem do woli zrywać owoce z każdego drzewa – z wyjątkiem jednego, które było drzewem zakazanym. Teoretycznie nie było nic łatwiejszego niż wieść dalej to dostatnie i stabilne życie, przestrzegając ustalonych zasad i reguł.

Nawet gdy pogodziłem się już z ryzykiem, z jakim wiązała się rola demaskatora, wciąż nie mogłem się z tą myślą oswoić. Zadawałem sobie pytania: Kim jestem, by samodzielnie podejmować decyzję o ujawnieniu poufnych informacji opinii publicznej? Kto dał mi mandat do bycia dysponentem państwowych tajemnic?

Informacje o tajnej polityce masowej inwigilacji, które zamierzałem ujawnić, były tak szokujące, że mogły spotkać się z niedowierzaniem, a zarazem miały na tyle specjalistyczny charakter, że mogły zostać niezrozumiane. Dlatego kiedy podjąłem ostateczną decyzję o ich

upublicznieniu, postanowiłem ujawnić także związaną z nimi dokumentację. Aby zdemaskować istnienie tajnego programu, wystarczyło po prostu poinformować o nim opinię publiczną, ale do wyjawienia programowego charakteru tajnych działań rządowych agencji niezbędne było opisanie ich mechanizmu i zasad funkcjonowania. To zaś wymagało przedstawienia konkretnych dokumentów, na przykład należących do NSA plików – tylu, ile było konieczne, by ukazać skalę nadużyć władzy. Miałem przy tym świadomość, że upublicznienie nawet jednego pliku PDF może skończyć się dla mnie wyrokiem więzienia.

Z powodu groźby rządowych sankcji wobec podmiotu czy platformy, za których pośrednictwem moje informacje ujrzałyby światło dzienne, przez pewien czas rozważałem opublikowanie materiałów na własną rękę. Takie rozwiązanie byłoby najwygodniejsze i najbezpieczniejsze: wystarczyło zgromadzić dokumenty potwierdzające zasadność moich obaw dotyczących rządowej inwigilacji obywateli i umieścić je w sieci, a następnie podać do publicznej wiadomości odpowiedni link. Jednym z powodów, dlaczego nie zdecydowałem się na taki krok, była kwestia uwierzytelnienia. Mnóstwo ludzi zamieszcza w internecie „tajne informacje” – wiele z nich dotyczy machin umożliwiających podróżowanie w czasie albo kontaktów z kosmitami. Zdawałem sobie sprawę z sensacyjnego charakteru doniesień i nie chciałem, żeby zostały wrzucone do jednego worka z rojeniami rozmaitych dziwaków i zniknęły pośród całej masy obłąkańczych teorii.

Szybko zrozumiałem, że w moim własnym interesie, a także w interesie opinii publicznej leży znalezienie osoby lub instytucji mogącej poręczyć za wiarygodność dokumentów, które zamierzałem ujawnić. Zależało mi również na tym, by mieć partnera, który byłby w stanie dokonać miarodajnej oceny potencjalnych zagrożeń związanych z ujawnieniem ściśle tajnych dokumentów, a także pomóc mi wyjaśnić opinii publicznej

wagę i znaczenie zawartych informacji, osadzając je we właściwych kontekstach technologicznym i prawnym. Byłem przekonany, że poradzę sobie z przedstawieniem, a nawet z analizą problemów, jakie rodziła masowa inwigilacja, ale jeśli chodziło o propozycje ich rozwiązania, musiałem zdać się na innych. Moja pogłębiająca się z biegiem lat nieufność w stosunku do instytucji wcale nie przekładała się na przekonanie, że sam byłbym w stanie skutecznie pełnić taką funkcję. Współpraca z takim czy innym podmiotem medialnym z jednej strony zabezpieczyłaby mnie przed najpoważniejszymi oskarżeniami, czyli przed zarzutem zdrady, a z drugiej strony pozwoliłaby wychwycić i wyeliminować wszelkie przejawy moich uprzedzeń, świadomych lub nieświadomych, osobistych albo zawodowych. Chciałem uniknąć sytuacji, w której moje polityczne poglądy wpłynęłyby na sposób przedstawienia lub na społeczny odbiór ujawnionych informacji. W końcu w kraju, gdzie wszyscy są inwigilowani, inwigilacja jest czymś najbardziej bezstronnym.

Z perspektywy czasu widzę wyraźnie, że moje dążenie do przekazania ujawnianych informacji nieskażonych własnymi ideologicznymi naleciałościami przynajmniej częściowo było zasługą korzystnego wpływu, jaki wywarła na mnie Lindsay. Przez wiele lat cierpliwie oswajała mnie z myślą, że niektóre moje opinie i obawy nie są podzielane ani przez nią, ani tym bardziej przez resztę świata. Uświadamiała mi, że dzieląc się z innymi moją wiedzą, nie mam prawa wymagać od nikogo przyjęcia mojego punktu widzenia. Że nie każda osoba sprzeciwiająca się naruszaniu prywatności gotowa jest stosować na co dzień 256-bitowe klucze szyfrujące albo zupełnie zrezygnować z korzystania z internetu. I że sprzeciw wobec nieuprawnionych działań władzy może wynikać z wielu różnych pobudek: dla jednej osoby może to być fakt pogwałcenia konstytucji, dla innej zaś pogwałcenie jej prywatności albo prywatności małżonka lub dzieci.

Lindsay była dla mnie kluczem do zrozumienia fundamentalnej prawdy, że różne motywy i metody nie utrudniają, lecz ułatwiają osiągnięcie wspólnych celów. Nieświadomie zachęciła mnie do przezwyciężenia moich zahamowań i poszukania pomocy u innych.

Tylko kim mieli być ci inni? Dzisiaj mało kto o tym pamięta, a nawet mało kto potrafi to sobie wyobrazić, ale kiedy zaczęła we mnie kiełkować myśl o ujawnieniu informacji na temat masowej inwigilacji, większość sygnalistów, chcących ujawnić nadużycia władzy, robiła to za pośrednictwem witryny WikiLeaks. Jej ówczesny sposób działania pod wieloma względami przypominał model operowania tradycyjnych wydawców prasy; jedną z zasadniczych różnic był radykalnie niechętny stosunek WikiLeaks do władzy państwowej. WikiLeaks regularnie współpracowało z redakcjami najbardziej uznanych gazet na świecie, takich jak „The Guardian”, „The New York Times”, „Der Spiegel”, „Le Monde” czy „El País”, publikując wspólnie z nimi dokumenty dostarczane przez informatorów. Owoce, jakie przynosiła ta współpraca w latach 2010–2011, utwierdziły mnie w przekonaniu, że WikiLeaks było najbardziej wartościowym pośrednikiem pomiędzy informatorami a dziennikarzami, a także najlepszą zaporą, chroniącą anonimowość źródeł.

Metoda działania WikiLeaks uległa jednak diametralnej zmianie po opublikowaniu informacji ujawnionych przez szeregową amerykańskiej armii Chelsea Manning; było to mnóstwo raportów z wojen w Iraku i w Afganistanie, a także amerykańskich depesz dyplomatycznych. Gwałtowna reakcja amerykańskiego rządu oraz pojawiające się w mediach krytyczne opinie na temat tego, jak WikiLeaks zredagowało przekazane przez Manning materiały, skłoniły zespół witryny do podjęcia decyzji o publikowaniu wszystkich przyszłych przecieków w takiej formie, w jakiej zostaną dostarczone przez informatorów: bez żadnych poprawek

i ingerencji redakcji. Ten zwrot w kierunku pełnej przejrzystości sprawił, że straciłem zainteresowanie publikacją moich informacji za pośrednictwem WikiLeaks. Nie różniłoby się to w zasadzie od opublikowania ich w sieci na własną rękę, a takie niewystarczające rozwiązanie odrzuciłem już wcześniej. Wiedziałem, że wyłaniająca się z dokumentów NSA historia rozwijanego w najgłębszej tajemnicy globalnego systemu masowej inwigilacji była tak zagmatwana i naszpikowana technicznymi szczegółami, że nie miało sensu przedstawiać jej opinii publicznej w postaci „sterty dokumentów". Tego rodzaju materiały wymagały cierpliwej i starannej redakcji, przeprowadzonej przez profesjonalnych dziennikarzy, najlepiej przy wsparciu wielu niezależnych instytucji prasowych.

Kiedy już postanowiłem, że ujawnię moje informacje bezpośrednio dziennikarzom, poczułem ulgę, ale wciąż nie mogłem pozbyć się pewnych obiekcji. Obawiałem się prestiżowych amerykańskich czasopism, a zwłaszcza najbardziej znanego i szanowanego tytułu w Stanach Zjednoczonych, czyli „New York Timesa". Za każdym razem, gdy myślałem o skontaktowaniu się z redakcją tej gazety, nachodziły mnie wątpliwości. Co prawda „New York Times" wykazywał pewną gotowość do narażenia się rządowi Stanów Zjednoczonych, publikując raporty WikiLeaks, ale miał też w historii mniej chlubną kartę, związaną z artykułem Erica Lichtblaua i Jamesa Risena poświęconym rządowemu programowi podsłuchiwania telefonicznych rozmów obywateli bez nakazu sądowego.

Lichtblau i Risen połączyli przekazy uzyskane od sygnalistów z Departamentu Sprawiedliwości z informacjami zdobytymi w toku własnego śledztwa dziennikarskiego i w ten sposób wpadli na trop jednego z aspektów operacji STELLARWIND – pierwszego programu masowej inwigilacji, jaki NSA wdrożyła po 11 września 2001 roku. Całą sprawę

opisali w obszernym i starannie udokumentowanym artykule. W połowie 2004 roku tekst był gotowy do druku i Bill Keller, redaktor naczelny, przedstawił go do wglądu administracji rządowej – była to rutynowa procedura, której celem było zapoznanie się przez redakcję z ewentualnymi argumentami strony rządowej, dlaczego publikacja może narazić na szwank bezpieczeństwo kraju. Również i tym razem, podobnie jak w większości wypadków, rząd nie podał żadnego konkretnego powodu sceptycznej oceny materiału, a jedynie dał do zrozumienia, że powody takie istnieją, ale objęte są tajemnicą państwową. Przedstawiciele rządu Busha oznajmili Kellerowi oraz Arthurowi Sulzbergerowi, wydawcy „New York Timesa", że opublikowanie informacji o podsłuchiwaniu obywateli Stanów Zjednoczonych bez zgody sądu rozzuchwali wrogów Ameryki i zwiększy zagrożenie ze strony terrorystów. Chociaż stwierdzeń tych nie poparto żadnymi dowodami, redakcja gazety dała się przekonać i artykuł Lichtblaua i Risena został wycofany z druku. Ostatecznie ukazał się na łamach „New York Timesa" dopiero ponad rok później, w grudniu 2005 roku, dzięki naciskom Risena, który zapowiedział, że wszystkie zawarte w artykule informacje znajdą się w przygotowywanej przez niego książce. Gdyby artykuł ukazał się od razu po jego napisaniu, mógłby wpłynąć na wynik wyborów prezydenckich w 2004 roku.

Gdyby „New York Times" albo inna gazeta wycięła mi podobny numer – czyli wykorzystała moje informacje do napisania artykułu, przedstawiła rezultat do wglądu organom rządowym, a następnie wycofałaby się z publikacji – byłoby po mnie. Biorąc pod uwagę wysokie prawdopodobieństwo zidentyfikowania mnie, informatora gazety, zostałbym zdemaskowany, zanim jakiekolwiek informacje trafiłyby do opinii publicznej.

Skoro nie mogłem zaufać powszechnie szanowanej gazecie, to czy mogłem obdarzyć zaufaniem jakąkolwiek inną instytucję? Zacząłem zadawać sobie pytanie, po co w ogóle się w to angażuję. Przecież nie na to się pisałem. Chciałem mieć fajną pracę, zajmować się komputerami i przy okazji zrobić coś pożytecznego dla mojego kraju. Wynajmowałem dom, byłem szczęśliwie zakochany, a mój stan zdrowia uległ poprawie. Każdy znak „stop”, jaki mijałem w drodze do pracy, był niczym symboliczne ostrzeżenie: zatrzymaj się, póki nie jest za późno, nie brnij w to szaleństwo. Moje serce walczyło z rozumem, a jedynym stale towarzyszącym mi uczuciem była rozpaczliwa nadzieja, że znajdzie się ktoś, kto bez mojego udziału dojdzie do właściwych wniosków i odkryje prawdę. Przecież na tym powinno polegać prawdziwe dziennikarstwo: na podążaniu za okruchami informacji i na łączeniu faktów. Czy nie tym właśnie zajmowali się na co dzień dziennikarze, prócz tego, że udzielali się na Twitterze?

Sęk w tym, że co do przedstawicieli czwartej władzy można było być pewnym dwóch rzeczy: tego, że zawsze gotowi są gonić za sensacją oraz że nie mają bladego pojęcia o nowoczesnej technice. Właśnie ten brak wiedzy z zakresu współczesnych technologii, a nawet zainteresowania tą dziedziną sprawił, że dziennikarze zupełnie zignorowali dwa wydarzenia, na które zwróciłem uwagę podczas zbierania informacji na temat masowej inwigilacji.

Pierwszym z nich było wydanie przez NSA komunikatu o rozpoczęciu budowy ogromnego centrum danych w miejscowości Bluffdale w stanie Utah. Agencja początkowo nazwała tę placówkę Massive Data Repository (repozytorium danych masowych), dopóki ktoś ze smykałką do PR-u nie zwrócił uwagi na fakt, że gdyby taka nazwa wyciekła do wiadomości publicznej, mogłyby się pojawić kłopotliwe pytania o zasadność masowego gromadzenia informacji. Ośrodek przemianowano więc na Mission Data

Repository (repozytorium danych zadaniowych) – akronim pozostał bez zmian, dzięki czemu nie trzeba było zmieniać slajdów wykorzystywanych podczas odpraw i zebrań. Na terenie MDR miały powstać cztery wypełnione serwerami hale, każda o powierzchni niemal dwóch i pół tysiąca metrów kwadratowych. Można tam było przechowywać gigantyczne ilości danych – w zasadzie to kronikę bieżącego życia całej ludzkości, o ile da się zrozumieć to życie poprzez powiązanie płatności z płatnikami, osób z ich aparatami telefonicznymi, aparatów telefonicznych z wykonywanymi połączeniami, połączeń z sieciami teleinformatycznymi, a także poprzez dane dotyczące wszelkich form internetowej aktywności prowadzonych za pośrednictwem tychże sieci.

Jedynym naprawdę znanym dziennikarzem, który zainteresował się komunikatem NSA, był James Bamford. W marcu 2012 roku opublikował na ten temat artykuł w miesięczniku „Wired". Wkrótce potem wzmianki dotyczące MDR ukazały się także w kilku pismach niezwiązanych z branżą technologiczną, ale żaden reporter nie pokusił się o dogłębne zbadanie tej sprawy. Nikt nie zadał pytań, które – przynajmniej w mojej ocenie – miałyby naprawdę fundamentalne znaczenie: Dlaczego agencja rządowa, a zwłaszcza agencja wywiadowcza, potrzebuje aż tak wielkiej przestrzeni? Jakie dane i jak długo zamierza tam przechowywać? Budowa tak ogromnego kompleksu nie miała sensu, chyba że planowano składować tam absolutnie wszystko i po wieczne czasy. Kompleks w Bluffdale sam w sobie stanowił *corpus delicti* – oczywisty dowód rzeczowy na łamanie prawa przez NSA. W samym środku pustyni powstał gigantyczny kompleks betonowych bunkrów, otoczony drutem kolczastym i wieżami strażniczymi, wyposażony we własną sieć energetyczną, z której pobierał tyle energii elektrycznej, co całe miasto. I nikt na to wszystko nie zwracał uwagi.

Drugie pominięte przez dziennikarzy wydarzenie miało miejsce rok później, w marcu 2013 roku – tydzień po zeznaniach złożonych przed senacką komisją do spraw wywiadu przez Jamesa Clappera, który okłamał przedstawicieli Kongresu, a oni puścili mu to płazem. W kilku czasopismach pojawiły się relacje z przesłuchania Clappera, jednak autorzy artykułów ograniczyli się do bezrefleksyjnego zacytowania jego zapewnień, że NSA nie zbiera dużych ilości danych na temat obywateli Stanów Zjednoczonych. Żadne media z tak zwanego mainstreamu nie odnotowały natomiast rzadkiego wydarzenia, jakim było publiczne wystąpienie Iry „Gusa" Hunta, szefa centralnego działu technicznego CIA.

Miałem okazję poznać Gusa w czasach, kiedy firma Dell oddelegowała mnie do CIA. Gus był jednym z naszych najważniejszych klientów. Wszyscy dostawcy usług i sprzętu dla CIA uwielbiali jego niedyskrecję. Mogłeś być pewien, że Gus zawsze powie ci więcej, niż powinien. Dla ludzi z działów sprzedaży Gus był niczym gadatliwy worek z pieniędzmi. W marcu 2013 roku Gus pojawił się w charakterze gościa specjalnego oraz mówcy na odbywającej się w Nowym Jorku konferencji GigaOM Structure Data. Była to cywilna impreza i żeby wziąć w niej udział, wystarczyło kupić bilet wstępu za jedyne 40 dolarów. Wystąpienia najważniejszych prelegentów, w tym także Gusa, można było obejrzeć na żywo i zupełnie za darmo w internecie.

Zależało mi na wysłuchaniu tego, co będzie miał do powiedzenia Gus, ponieważ z wewnętrznych kanałów informacyjnych NSA dowiedziałem się, że CIA podjęła w końcu decyzję w sprawie umowy na przetwarzanie danych w chmurze. Oferta przygotowana przez mój dawny zespół Della została odrzucona, podobnie jak propozycja HP. Dziesięcioletni kontrakt o wartości sześciuset milionów dolarów przypadł ostatecznie firmie Amazon i to ona miała zająć się stworzeniem i zarządzaniem usługami

chmurowymi dla CIA. Nie było mi z tego powodu przykro – wręcz przeciwnie, ucieszyłem się, że agencja nie będzie wykorzystywać efektów mojej pracy. Z czystej zawodowej ciekawości chciałem się jednak przekonać, czy na konferencji Gus wspomni o podpisaniu umowy z Amazonem, a także o powodach, dlaczego wybrano ofertę akurat tego przedsiębiorstwa – krążyły bowiem pogłoski, że przetarg był nie do końca uczciwy, ponieważ jego warunki faworyzowały właśnie Amazona.

Wystąpienie Gusa faktycznie okazało się wyjątkowo interesujące, chociaż z zupełnie nieoczekiwanych powodów. Miałem okazję być świadkiem, jak najwyższy rangą urzędnik agencji do spraw technicznych stoi na scenie w pomiętym garniturze i opowiada zebranym na widowni i nieposiadającym certyfikatu dostępu do informacji niejawnych cywilom – a za pośrednictwem internetu także całemu światu – o celach i możliwościach technicznych agencji. Żarty, którymi Gus przeplatał wywody, były prawie tak słabe jak jego znajomość obsługi PowerPointa, ale ja i tak słuchałem go z wielkim zainteresowaniem – i rosnącym zdumieniem.

„W CIA – oświadczył Gus – staramy się zbierać wszelkie możliwe dane i zachować je na zawsze”. Jakby tego było mało, dodał: „Jesteśmy bardzo blisko tego, by móc przetwarzać wszystkie informacje generowane przez człowieka”. Podkreślenie było dziełem Gusa. Odczytywał tekst swojego wystąpienia z wyświetlanych na ekranie slajdów: brzydkie zdania zapisane były brzydką czcionką i zilustrowane utrzymanymi w czterobarwnej kolorystyce clipartami – nieodłącznym elementem każdej prezentacji przygotowanej przez urzędnika rządowego.

Wśród słuchaczy znajdowało się kilkoro dziennikarzy, przy czym niemal wszyscy byli pracownikami rządowych periodyków technicznych w rodzaju „Federal Computer Week”. Znamienny był fakt, że Gus pod

koniec wystąpienia postanowił odpowiedzieć na pytania z sali. Dokładniej mówiąc, była to nie tyle sesja pytań i odpowiedzi, co raczej dodatkowa prezentacja, adresowana bezpośrednio do przedstawicieli prasy. Odniosłem wrażenie, że Gus próbuje zrzucić ciężar z piersi – i nie chodziło bynajmniej o jego idiotyczny krawat.

Gus powiedział dziennikarzom, że CIA jest w stanie namierzyć ich smartfony, nawet kiedy są wyłączone – i może monitorować całą ich komunikację. Nie zapominajmy, że kierował te słowa do amerykańskich dziennikarzy. A fraza „może monitorować" zabrzmiała w jego ustach jak „monitorowała", „monitoruje" i „będzie monitorować". Gus perorował w niespokojny i dość niepokojący sposób; takie zachowanie było niepodobne do wysokiego dostojnika CIA. „Technologia gna dziś naprzód tak szybko, że ani rząd, ani prawo nie są w stanie za nią nadążyć – stwierdził. – Postęp technologiczny jest szybszy od każdego z nas: dlatego powinniście zadać sobie pytanie, jakie macie prawa i w czyim posiadaniu znajdują się wasze dane". Zamurowało mnie. Gdyby podobny wykład wygłosił ktoś niższy rangą od Gusa, jeszcze tego samego dnia musiałby przywdziać pomarańczowy więzienny uniform.

Relacja z publicznej spowiedzi Gusa pojawiła się tylko na stronie Huffington Post. Ale wideo z wystąpieniem trafiło na YouTube'a i pozostawało tam przez sześć kolejnych lat, przynajmniej do dnia, w którym pisałem te słowa. Kiedy ostatnio sprawdzałem, miało 313 wyświetleń. Ja sam obejrzałem je kilkanaście razy.

Wyciągnąłem z tego następującą lekcję: jeśli chciałem skutecznie ujawnić tajne informacje, to nie mogłem tylko wręczyć pliku dokumentów kilku dziennikarzom; nawet gdybym pomógł im w ich interpretacji, to wciąż byłoby za mało. Musiałem stać się partnerem reporterów, dostarczyć odpowiednie narzędzia techniczne i nauczyć ich, jak z nich korzystać –

tylko wtedy będą mogli bezpiecznie i precyzyjnie poinformować opinię publiczną o wszystkich istotnych faktach. To zaś oznaczało, że musiałem zaangażować się w pełni i bez reszty w jedno z najpoważniejszych przestępstw, jakie może popełnić pracownik wywiadu: o ile inni przeniewiercy dopuszczali się szpiegostwa na rzecz obcych służb, działalności wywrotowej i zdrady, ja miałem dopuścić się podżegania i pomocy w działaniach dziennikarskich. Z punktu widzenia przepisów prawa wszystkie te przestępstwa są w zasadzie równoważne. Amerykańskie prawo nie czyni rozróżnienia między przekazaniem tajnych informacji przedstawicielom prasy w interesie publicznym a oddaniem czy nawet sprzedaniem ich wrogowi. Podczas mojego pierwszego szkolenia formacyjnego spotkałem się z nieco inną opinią na ten temat: powiedziano nam wówczas, że sprzedanie państwowych tajemnic przedstawicielom obcego wywiadu to zbrodnia nieco mniejszego kalibru niż przekazanie ich za darmo reporterowi. Dziennikarz bowiem opublikuje otrzymane materiały, natomiast wrogi wywiad najprawdopodobniej nie podzieli się zdobyczą z nikim, nawet z sojusznikami.

Zważywszy na podejmowane przeze mnie ryzyko, musiałem znaleźć takich partnerów, którym mógłbym zaufać i którzy sami cieszyli się zaufaniem opinii publicznej. Musieli to być dziennikarze sumienni, a jednocześnie dyskretni, niezależni, a przy tym wiarygodni. Powinni być na tyle bezkompromisowi, by nie zawahali się zakwestionować moich podejrzeń i domniemań, jeśli uznają, że nie są one poparte twardymi dowodami, a także by mieli odwagę odeprzeć oskarżenia rządu, kiedy ten bezpodstawnie zarzuci im narażanie na szwank życia amerykańskich obywateli. Przede wszystkim jednak musiałem mieć pewność, że wybrane przeze mnie osoby nie ugną się pod presją władz, która – nie miałem co do

tego wątpliwości – będzie silniejsza i dotkliwsza od tego, czego do tej pory doświadczyliśmy zarówno ja, jak i moi partnerzy.

Zakroiłem moje poszukiwania nie na tyle szeroko, by narazić misję na niebezpieczeństwo, lecz jednocześnie wystarczająco szeroko, żeby jedno niepowodzenie nie oznaczało fiaska – chciałem uniknąć sytuacji analogicznej do zablokowania publikacji artykułu Lichtblaua i Risena na łamach „New York Timesa". Wiedziałem, że jeden dziennikarz, jedna gazeta, a nawet jeden kraj publikacji to za mało, by sprostać determinacji, z jaką rząd Stanów Zjednoczonych stara się powstrzymywać ujawnianie niewygodnych materiałów. Uznałem, że najlepiej byłoby przekazać jednocześnie wszystkim wybranym dziennikarzom pełen komplet dokumentów, nie zostawiając sobie niczego w zanadrzu. Dzięki temu uwaga władz nie skupiłaby się na mnie, tylko na wielu różnych osobach, a ja miałbym gwarancję, że prawda ujrzy światło dzienne, nawet gdybym został aresztowany.

Zawężając stopniowo listę potencjalnych partnerów, uświadomiłem sobie, że podszedłem do zadania w niewłaściwy sposób. Zamiast próbować samemu wybrać odpowiednich dziennikarzy, powinienem pozwolić, by zrobił to za mnie system, który zamierzałem zdemaskować. Doszedłem do wniosku, że najlepszymi partnerami będą dla mnie ci dziennikarze, którzy ze względu na swoją działalność zawodową znaleźli się na celowniku organów bezpieczeństwa państwa.

Laura Poitras, dokumentalistka, skupiała się na problemach związanych z polityką zagraniczną Stanów Zjednoczonych po 11 września 2001 roku. W filmie *Mój kraju!* przedstawiła okoliczności irackich wyborów, które odbyły się w 2005 roku pod amerykańską okupacją. Bohaterem innego jej dokumentu, zatytułowanego *The Program*, był William Binney, kryptoanalityk NSA. Korzystając z odpowiednich kanałów komunikacji

wewnętrznej i zewnętrznej, Binney zgłaszał przełożonym i politykom zastrzeżenia dotyczące naruszania prywatności obywateli przez program TRAILBLAZER, poprzednika programu STELLARWIND. Władze zarzuciły Binneyowi ujawnienie tajnych informacji, poddały go licznym represjom, a w końcu nasłały na niego uzbrojonych funkcjonariuszy, którzy aresztowali go w jego własnym domu; mimo to Binney nigdy nie został formalnie postawiony w stan oskarżenia. Laura sama padała ofiarą nękania przez władze i za każdym razem, gdy przekraczała granicę Stanów Zjednoczonych, była zatrzymywana i przesłuchiwana przez funkcjonariuszy straży granicznej.

Glenn Greenwald to prawnik zaangażowany w obronę swobód obywatelskich; został felietonistą i komentatorem politycznym. Felietony publikował początkowo w portalu Salon – jako jeden z nielicznych autorów pisał w 2009 roku o odtajnionej wersji raportu inspektora generalnego na temat działalności NSA – a potem na łamach amerykańskiego wydania „Guardiana”. Lubiłem go za sceptyczne podejście i zadziorne pióro; Glenn to taki człowiek, który gotów jest walczyć choćby z diabłem, a jeśli diabła nie ma akurat pod ręką, to będzie wadził się z samym sobą. Ewen MacAskill z brytyjskiego „Guardiana” i Bart Gellman z „Washington Postu” okazali się lojalnymi i cennymi partnerami (a także cierpliwymi przewodnikami po dziennikarskiej dżungli), ale najwcześniej nawiązałem więź z Laurą i Glennem – być może dlatego, że oboje interesowali się nie tylko opisaniem nadużyć amerykańskich agencji wywiadowczych, ale także z osobistych pobudek pragnęli zrozumieć zasady i metodę funkcjonowania tych instytucji.

Kiedy już wybrałem przyszłych partnerów, pozostało mi znaleźć sposób na nawiązanie z nimi kontaktu.

Nie mogłem ujawnić mojego nazwiska, dlatego kontaktowałem się z dziennikarzami pod różnymi pseudonimami – maskami, jakie nosiłem przez pewien czas, by następnie zastąpić je innymi. Moim pierwszym pseudonimem był „Cincinnatus” od imienia słynnego rzymskiego konsula, który dobrowolnie zrzekł się urzędu i władzy, po czym powrócił do pracy na roli. Kolejnym moim kryptonimem był „Citizenfour”. Niektórzy dziennikarze uznali, że wybrałem go, ponieważ uważałem się za czwartego – po Binneyu i jego dwóch kolegach, Kirku Wiebe i Edzie Loomisie, którzy wspólnie ujawnili nieprawidłowości związane z programem TRAILBLAZER – dysydenta, jaki w ostatnich latach pojawił się w szeregach NSA. Mój pseudonim faktycznie nawiązywał do trzech wcześniejszych demaskatorów; w rzeczywistości jednak miałem na myśli Thomasa Drake’a, który przekazał dziennikarzom informację o istnieniu programu TRAILBLAZER, a także Daniela Ellsberga i Anthony’ego Russo, którzy ujawnili treść tajnego rządowego raportu, tak zwanego Pentagon Papers, zawierającego nieznane opinii publicznej informacje na temat amerykańskiego zaangażowania w Wietnamie i tym samym przyczynili się do zakończenia wojny. Ostatnią ksywką, którą podpisywałem wiadomości wysyłane do moich partnerów, był „Verax”, czyli łaciński termin oznaczający „mówiącego prawdę”. Wybrałem go, ponieważ chciałem, by moje działania stanowiły alternatywę dla metod hakera o pseudonimie „Mendax” („kłamca”) – pod tym przydomkiem ukrywał się młody Julian Assange, później twórca portalu WikiLeaks.

Nie będziesz w stanie pojąć, jak trudno jest zachować anonimowość w sieci, dopóki nie spróbujesz ukrywać tożsamości tak, jakby zależało od tego twoje życie. Większość systemów komunikacji wykorzystywanych w agencjach wywiadowczych ma jeden podstawowy cel: sprawić, by postronny obserwator wymiany informacji nie zdołał poznać prawdziwej

tożsamości jej uczestników ani nie przypisał im związku z daną agencją. Dlatego takie metody komunikacji określa się mianem „nieprzypisywalnych”. Dzięki filmom i serialom wszyscy znamy szpiegowskie metody zachowania anonimowości stosowane przed nastaniem ery internetu: adresy bezpiecznych kryjówek zakodowane w graffiti na ścianie kabiny w publicznej toalecie albo w formie skrótów użytych w drobnym ogłoszeniu w gazecie. Albo tak zwane martwe skrzynki kontaktowe z okresu zimnej wojny – dyskretne znaki wykonane kredą na skrzynce pocztowej, informujące o tym, że w wydrążonym pniu drzewa w parku czeka na odbiór tajna przesyłka. Nowoczesną wersją tych metod mogą być na przykład fałszywe profile wymieniające się fałszywymi informacjami na czacie na portalu randkowym albo – znacznie częściej – pozornie niewinna aplikacja, za której pomocą można pozostawić pozornie niewinną wiadomość na pozornie niewinnym serwerze Amazona, kontrolowanym sekretnie przez CIA. Ja jednak potrzebowałem czegoś jeszcze lepszego, co nie wymagałoby ponoszenia tak dużych kosztów, a zarazem ograniczało ryzyko demaskacji.

Postanowiłem, że będę korzystał z cudzego łącza internetowego. Teoretycznie wystarczyłoby wejść do McDonalda lub Starbucksa i zalogować się do darmowego Wi-Fi. Niestety nie było to takie proste. W barach i kawiarniach są kamery monitoringu, paragony, a do tego mnóstwo ludzi, którym można zapaść w pamięć. Co więcej, wszystkie urządzenia umożliwiające bezprzewodowy dostęp do internetu, od telefonów po laptopy, posiadają unikatowe identyfikatory w postaci adresu MAC (Machine Address Code), a one pozostawiają ślady w każdym punkcie dostępu Wi-Fi, gdzie urządzenie łączy się z internetem; na podstawie tych śladów można ustalić miejsca pobytu, a nawet odtworzyć trasę przemieszczania się użytkownika danego urządzenia.

Dlatego zamiast udać się do McDonalda czy Starbucksa, wybrałem się na przejażdżkę. Ściślej rzecz ujmując, wybrałem się na przejażdżkę w poszukiwaniu niezabezpieczonych sieci bezprzewodowych. Musiałem przerobić samochód na mobilny wykrywacz Wi-Fi – aby tego dokonać, wystarczy zaopatrzyć się w laptopa, antenę o dużej mocy i odbiornik GPS z magnesem, który można umieścić na dachu samochodu. Źródłem zasilania może być samochód, przenośna bateria albo sam laptop. Wszystko, czego ci potrzeba, zmieści się w małym plecaku.

Zabierałem ze sobą taniego laptopa z opartym na Linuksie „anonimizującym" systemem operacyjnym TAILS – w momencie wyłączenia komputera system ten zapomina o wszystkim, co do tej pory robiłeś. Po ponownym uruchomieniu urządzenia nie ma na nim żadnych logów ani innych śladów informacji pozostałych po poprzedniej sesji. TAILS pozwalał mi łatwo ukrywać adres MAC mojego laptopa – za każdym razem, gdy łączyłem się z siecią, pozostawiał w niej ślad należący do jakiegoś innego komputera, którego w żaden sposób nie można było ze mną powiązać. TAILS posiadał również wbudowane wsparcie połączeń z anonimową siecią Tor.

Wieczory i weekendy spędzałem na objazdach niemal całej wyspy O'ahu. Moja antena wyłapywała sygnały każdej sieci bezprzewodowej, a czujnik GPS oznaczał dokładne położenie wszystkich punktów dostępu do lokalnych sieci, wykrytych za pomocą programu Kismet. W rezultacie stworzyłem mapę niewidzialnych sieci mijanych nieświadomie każdego dnia. Skandalicznie wiele z nich w ogóle nie było zabezpieczonych lub posiadało zabezpieczenia, które z łatwością mogłem obejść. Niektóre sieci wymagały jednak zastosowania nieco bardziej wyrafinowanych metod. Blokowałem sieć, przerywając tym samym połączenia prawowitych użytkowników. Kiedy ich urządzenia próbowały ponownie się połączyć,

automatycznie wysyłały „pakiety uwierzytelniające” – pozostawało mi już tylko je przechwycić i odszyfrować hasła dostępowe, a dzięki nim mogłem zalogować się do danej sieci tak jak każdy inny „uprawniony” użytkownik.

Wyposażony w tę mapę sieci jeździłem po O’ahu w tę i we w tę, co jakiś czas logując się do skrzynki e-mailowej i sprawdzając, który z dziennikarzy mi odpisał. Po nawiązaniu kontaktu z Laurą Poitras niemal cały wieczór wymieniałem z nią wiadomości – siedziałem w samochodzie zaparkowanym przy plaży, pożyczając sobie Wi-Fi z ośrodka wypoczynkowego. Niektórych dziennikarzy musiałem przekonywać do korzystania z szyfrowanej poczty elektronicznej, co w 2012 roku nie było wcale takie proste. Niekiedy musiałem pokazać im, jak się to robi, dlatego wysyłałem przygotowane własnoręcznie samouczki przez sieć pobliskiej biblioteki. Albo szkoły. Lub banku – banki miały przerażająco słabe zabezpieczenia.

Pewnego dnia siedziałem w samochodzie na parkingu centrum handlowego. Czułem się bezpiecznie, mając świadomość, że wystarczy zamknąć laptopa, by nikt nie poznał moich sekretów. Pisałem robocze wersje manifestów, w których wyjaśniałem moje pobudki, ale ostatecznie wszystko skasowałem. Próbowałem też pisać e-maile do Lindsay, ale je również usunąłem. Nie potrafiłem znaleźć właściwych słów.

23_Odczytaj_Zapisz_Wykonaj|

Odczytaj, zapisz, wykonaj – w informatyce te hasła funkcjonują pod pojęciem uprawnień użytkownika. Określają zakres władzy nad komputerem lub siecią – co konkretnie użytkownik może, a czego nie może robić. Uprawnienie do odczytu zezwala na dostęp do zawartości pliku, uprawnienie do zapisu pozwala zawartość tę modyfikować, natomiast uprawnienie do wykonywania daje możliwość decydowania o tym, czy plik albo program będzie mógł przeprowadzić czynności, do których został stworzony.

Odczytaj, zapisz, wykonaj – do tego sprowadzał się mój prosty, trójetapowy plan. Chciałem dostać się do samego serca najlepiej zabezpieczonej sieci świata, by odkryć prawdę, następnie ją skopiować i wydobyć na światło dzienne. A wszystko to nie dając się złapać – nie pozwalając nikomu innemu, by odczytał i zapisał moje poczynania, a następnie wykonał na mnie wyrok.

Niemal wszystko, co robisz na komputerze albo innym urządzeniu cyfrowym, jest dokumentowane. Zasada ta najsilniej działa w NSA, gdzie każde zalogowanie do systemu i wylogowanie z niego jest odnotowywane w rejestrze. Za każdym razem, gdy korzystałem z moich uprawnień, zostawiałem po sobie ślad. Kiedy otwierałem albo kopiowałem dowolny plik, czynność ta była rejestrowana. Podobnie gdy pobierałem, przenosiłem i usuwałem dane – rejestr mojej aktywności aktualizował się o wykonane operacje. Istniały rejestry przepływu danych przez sieć oraz rejestry użytkowania infrastruktury wykorzystującej kryptografię klucza

publicznego – pracownicy żartowali, że kamery są zamontowane nawet w kabinach toaletowych. NSA prowadziła niemałą liczbę programów kontrwywiadowczych szpiegujących tych, którzy zajmowali się szpiegowaniem, i wystarczyłoby, żeby choć jeden z tych programów przyłapał mnie na robieniu czegoś, czego nie powinienem robić, a wymazane zostałyby nie tylko moje pliki.

Na szczęście ta sama cecha, która dawała systemom agencji siłę, była ich słabością: ogromna złożoność sprawiała, że w wielu wypadkach nawet osoby, które się nimi zajmowały, nie do końca wiedziały, w jaki sposób te systemy działają. W rzeczywistości prawie nikt nie zdawał sobie sprawy, w których obszarach nakładają się na siebie, a gdzie mają luki. Nikt, oczywiście poza administratorami. Wszystkie te skomplikowane systemy śledzące, które sobie wyobrażasz, te o groźnych nazwach jak MIDNIGHTRIDER… cóż, ktoś musi je instalować. NSA płaci za sieć, ale w rzeczywistości należy ona do sysadminów takich jak ja.

Faza Odczytu mojego planu przybrała zatem formę tańca pomiędzy nićmi cyfrowej sieci pułapek rozpiętymi na łączach spinających NSA z wszystkimi innymi agencjami wywiadowczymi, zarówno amerykańskimi, jak i zagranicznymi. (Należał do nich brytyjski partner NSA, Rządowa Centrala Łączności [Government Communications Headquarters, GCHQ]. Założyła ona między innymi sieć OPTICNERVE, która działała na platformach umożliwiających wideoczat w rodzaju Yahoo Messengera i co pięć minut zapisywała zrzut obrazu z kamery użytkownika, oraz PHOTONTORPEDO, program pobierający adresy IP użytkowników MSN Messengera). Użycie Heartbeatu do pobierania interesujących mnie dokumentów pozwoliło mi wykorzystać „masowe gromadzenie danych” do walki z tymi, którzy zwrócili te metody przeciw społeczeństwu. Przeistoczyłem aparaturę wywiadu w potwora jako żywo przypominającego

Frankensteina. Narzędzia bezpieczeństwa agencji odnotowywały tożsamość czytających dokumenty, ale nie miało to znaczenia: wszyscy, którym chciało się sprawdzać rejestry aktywności, zdążyli się już przyzwyczaić do szperania Heartbeatu. Aktywność programu nie wzbudzała niepokoju. Zapewniło mi to idealną przykrywkę.

Niestety Heartbeat posłużył tylko za narzędzie do przeniesienia plików – w o wiele za dużej ilości – na serwer na Hawajach, a jego rejestru aktywności nie mogłem obejść nawet ja. Potrzebowałem sposobu, by pracować na tych danych, przeszukiwać je i pozbywać się tych, które uznam za nieprzydatne, mało interesujące bądź zawierające wartościowe tajemnice państwowe, a ich nie zamierzałem ujawniać dziennikarzom. Na tym etapie fazy Odczytu wciąż czyhały na mnie różnorakie zagrożenia. Wynikało to w dużej mierze stąd, że musiałem zacząć mierzyć się z protokołami bezpieczeństwa nienastawionymi na monitoring, lecz na zapobieganie określonym działaniom. Gdybym wyszukiwał dane, które mnie interesowały, na serwerze Heartbeatu, w systemie zapaliłaby się ogromna czerwona lampa z poleceniem ARESZTUJCIE MNIE.

Rozmyślałem nad tą kwestią przez dłuższy czas. Byłem przekonany, że jeśli skopiuję pliki bezpośrednio z serwera Heartbeatu na osobisty nośnik pamięci i spróbuję wymaszerować z Tunelu jakby nigdy nic, zostanę złapany. Mogłem jednak zrobić coś innego – przenieść pliki bliżej wyjścia: przekierować je do stacji pośredniej.

Nie mogłem wysłać ich na jeden z komputerów, na których pracowaliśmy na co dzień, ponieważ po modernizacji zakończonej w 2012 roku wszystkie stacje robocze w Tunelu były tak zwanymi cienkimi klientami: bezbronnymi komputerkami o niewydolnych dyskach i procesorach, które nie mogły samodzielnie przechowywać ani przetwarzać danych; do potrzeb magazynowych i obliczeniowych wykorzystywały

chmurę. W zapomnianym zaułku biura stała jednak piramida nieużywanych komputerów stacjonarnych – niszczejących maszyn starszego typu; agencja pozbyła się ich po uprzednim usunięciu danych. Mówiąc o starszym typie, mam na myśli komputery, które dla każdego, kto nie dysponuje budżetem NSA, wydawałyby się nowoczesne. Były to pecety Della z lat 2009 i 2010, w dużych prostopadłościennych szarych obudowach o słusznej wadze. Mogły przechowywać i przetwarzać dane we własnym zakresie, bez łączenia się z chmurą. Szczególnie podobało mi się w nich to, że choć wciąż pozostawały zarejestrowane w systemie NSA, praktycznie nie dało się ich ściśle monitorować, póki ktoś nie podłączył ich do głównej sieci.

Mogłem łatwo uzasadnić korzystanie z tych solidnych, niezawodnych pudeł, sięgając po argument, że oto chciałem przekonać się, czy Heartbeat zadziała na starszych systemach operacyjnych. Nie wszystkie placówki NSA przeszły w pełni na nowe komputery i nie wszyscy pracownicy mieli do nich dostęp. A gdyby tak Dell chciał uruchomić cywilną wersję mojego oprogramowania? Albo jeśli zechcą z niego korzystać CIA, FBI bądź inna równie uwsteczniona organizacja? Testy kompatybilności dawały mi przykrywkę, pod którą mogłem przenosić pliki na stare komputery i tam przeszukiwać je, filtrować i organizować tak, jak dusza zapragnie, i tak długo, jak zachowywałem należytą ostrożność. Pewnego razu, niosąc jeden z tych starych olbrzymów do mojego biurka, minąłem jednego z dyrektorów działu informatycznego, akurat najgorętszego orędownika wymiany sprzętu. Zatrzymał mnie i spytał, do czego jest mi potrzebny ten stary rupieć.

– Do wykradania tajemnic – odpowiedziałem i obaj się roześmialiśmy.

Wraz z zakończeniem fazy Odczytu pliki, na których mi zależało, były zapisane w ładnie uporządkowanych folderach. Niestety na komputerach, które do mnie nie należały i znajdowały się pod ziemią, w Tunelu.

Powinienem zatem rozpocząć etap Zapisu, co oznaczało boleśnie powolny, nudny, a przy tym absolutnie przerażający proces kopiowania plików ze zdemobilizowanych Dellów na nośnik, który będę mógł niepostrzeżenie wynieść z budynku.

Najprościej i najbezpieczniej jest skopiować plik ze stacji roboczej w placówce wywiadu w najstarszy sposób: zrobić zdjęcie. W budynkach NSA obowiązuje, rzecz jasna, zakaz posiadania smartfonów, ale pracownicy co rusz wnoszą je przez przypadek i nikt tego nie zauważa. Zostawiają je w sportowych torbach albo w kieszeniach kurtek. Kiedy w trakcie losowego przeszukania zostają przyłapani, reagują speszeniem i głupkowatymi minami zamiast w panice krzyczeć po chińsku do swoich zegarków. Często otrzymują tylko ostrzeżenie, szczególnie jeśli jest to ich pierwsza wpadka.

Przemycenie smartfona pełnego tajemnic NSA na zewnątrz Tunelu było jednak bardziej ryzykownym gambitem. Bardzo prawdopodobne, że nikt nie zwróci uwagi – ani nie przejmie się – gdybym opuścił budynek z telefonem, i możliwe, że smartfon okazałby się odpowiednim narzędziem dla członka personelu, który chciałby skopiować pojedynczy raport z tortur. Nie zachwycał mnie jednak pomysł wykonywania tysięcy zdjęć ekranu swojego komputera w centrum ściśle tajnej placówki. Poza tym telefon musiałby być skonfigurowany tak, by podczas ewentualnego przeszukania nawet najwybitniejsi eksperci dochodzeniowi świata nie znaleźli niczego, czego tam być nie powinno.

Powstrzymam się od wyjawienia, w jaki konkretnie sposób dokonałem Zapisu – czyli kopiowania i szyfrowania danych – bo nie chcę, żeby NSA straciła prawo bytu. Wspomnę jednak, jaki nośnik wykorzystałem do wyniesienia skopiowanych plików. Zapomnij o pendrive’ach – są zbyt nieporęczne w stosunku do objętość danych, jaką mieszczą. Zamiast nich

posłużyłem się kartami pamięci SD (skrót od Secure Digital, czyli „bezpiecznych danych“), a właściwie ich zminiaturyzowanymi odmianami, kartami mini- i microSD.

Na pewno znasz te karty, jeśli kiedykolwiek korzystałeś z cyfrowego aparatu fotograficznego albo kamery lub potrzebowałeś więcej pamięci w tablecie. Stanowią cudowne osiągnięcie w dziedzinie nieulotnej pamięci flash: są cholernie maleńkie i przy wymiarach 20 na 21,5 milimetrów w wersji mini i 15 na 11 milimetrów w wersji micro (wielkość paznokcia małego palca u dłoni) niezwykle łatwe do ukrycia. Kartę taką można upchnąć, na przykład, w segmencie kostki Rubika i nikt tego nie zauważy. Wynosiłem je również w skarpetce, a także, w okresie najsilniejszej paranoi, pod policzkiem, żebym w razie czego mógł połknąć dowody. Później, kiedy nabrałem pewności siebie i ufności do metod szyfrowania, które stosowałem, po prostu wychodziłem z kartami na dnie kieszeni. Wykrywacze metalu prawie nigdy ich nie rejestrowały, a nikt normalny nie wątpił w moje tłumaczenie, że zupełnie zapomniałem o czymś tak drobnym.

Z rozmiarem kart SD wiąże się niestety jedna wada: ich zapis odbywa się niezwykle powoli. Przenoszenie ogromnych ilości danych zawsze trwa dłużej, niż byś chciał, a co dopiero kiedy kopiujesz je nie na szybki twardy dysk, lecz na maleńki krzemowy wafel zatopiony w plastiku. Ja zaś, co gorsza, nie tylko kopiowałem dane. Musiałem je również deduplikować, kompresować i szyfrować, a żadnego z tych procesów nie można było wykonywać jednocześnie z pozostałymi. Wykorzystywałem wszystkie umiejętności, których nabyłem podczas pracy z magazynami danych, bo w gruncie rzeczy wykonywałem swoje obowiązki: archiwizowałem magazyn danych NSA, przygotowując na zewnętrznym nośniku kopię zapasową dowodów nadużyć służb wywiadowczych.

Zapełnienie jednej karty zajmowało osiem godzin albo i dłużej – czyli cały dzień roboczy. I choć zacząłem znów przychodzić na nocną zmianę, trząsłem się ze strachu bez przerwy, kiedy stary komputer ze zgaszonym monitorem mielił dane w tle w wątłym świetle jedynej włączonej i w związku z nakazem oszczędzania prądu po godzinach przyciemnionej lampy w panelu podsufitowym. Od czasu do czasu włączałem monitor, żeby sprawdzić postęp i skrzywić się z niezadowoleniem. Na pewno znasz to koszmarne uczucie, kiedy wbijasz wzrok w pasek postępu pokazujący osiemdziesiąt cztery procent, potem osiemdziesiąt pięć… Pozostała jedna godzina, pięćdziesiąt osiem minut i pięćdziesiąt trzy sekundy… Kiedy pasek zbliżał się do przynoszących słodką ulgę stu procent, co oznaczało, że wszystkie pliki zostały skopiowane, z wyczerpania spływałem potem; wydawało mi się, że widzę przemieszczające się cienie i zza każdego rogu słyszę kroki.

Ostatni etap: Wykonaj. Po zapełnieniu wszystkich kart musiałem zrealizować mój plan ucieczki: wydobyć bezcenne archiwum z budynku, mijając szefów i wojskowe mundury, przechodząc po schodach, pustym korytarzem, przez skaner identyfikatora, obok uzbrojonych strażników i przez śluzy – strefy bezpieczeństwa, gdzie drzwi zamykają ci się za plecami, a te przed tobą nie otwierają się, dopóki system nie potwierdzi twojej tożsamości; jeśli z identyfikatorem jest coś nie tak lub nie zgadza się jeszcze coś innego, strażnicy wyciągają broń, drzwi zatrzaskują się i stwierdzasz w myślach: „Jezu, ale się wkopałem”. To na tym etapie – tak wynikało ze wszystkich raportów, które przeczytałem, i tak było we wszystkich koszmarach, które mi się śniły – mieli mnie złapać. Miałem tego pewność. Za każdym razem, gdy wychodziłem, byłem odrętwiały z przerażenia. Zmuszałem się, żeby nie myśleć o karcie pamięci, bo kiedy

jest obecna w myślach, człowiek zachowuje się inaczej niż zwykle – podejrzanie.

Nieoczekiwanym pozytywnym skutkiem poznania metod inwigilacji stosowanych przez NSA było to, że zyskałem również lepsze pojęcie o niebezpieczeństwach, które na mnie czyhały. Innymi słowy, poznając systemy agencji, nauczyłem się, jak nie dać się im złapać. Moimi przewodnikami w tej dziedzinie stały się akty oskarżenia wniesione przez rząd przeciw byłym agentom – w dużej mierze prawdziwym gnojkom, którzy, posługując się żargonem wywiadu, „ewakuowali" niejawne informacje dla zysku. Skompilowałem wszystkie akty oskarżenia, jakie udało mi się znaleźć, i przestudiowałem je. Dla FBI – agencji zajmującej się wszystkimi przestępstwami wewnątrz wywiadu – ogromne źródło dumy stanowiły objaśnienia, jak konkretnie łapie podejrzanych, i wierz mi, nie miałem zupełnie nic przeciwko korzystaniu z tych doświadczeń. Zwróciłem uwagę, że niemal we wszystkich przypadkach FBI czekało z aresztowaniem aż do chwili, gdy podejrzany zakończył pracę i szykował się do powrotu do domu. Czasami agenci pozwalali mu wynieść materiały z SCIF (Sensitive Compartmented Information Facility) – placówki upoważnionej do obróbki danych o szczególnej wrażliwości, czyli budynku albo pomieszczenia zabezpieczonego przed działalnością wywiadowczą – w miejsce publiczne, gdzie samo posiadanie takich danych to przestępstwo federalne. Regularnie wyobrażałem sobie oddział agentów FBI zaczajony na mnie bezpośrednio za wyjściem z Tunelu, w świetle dnia, na widoku innych.

Zwykle starałem się nawiązać niezobowiązującą rozmowę ze strażnikami. Tu właśnie przychodziła mi z największą pomocą kostka Rubika. Byłem znany strażnikom i wszystkim pozostałym pracownikom Tunelu jako chłopak z kostką Rubika, ponieważ bawiłem się nią, kiedy szedłem korytarzem. Nabrałem takiej wprawy, że potrafiłem ją ułożyć jedną

ręką. Stała się moim totemem, nieodłączną zabawką i narzędziem odwracania uwagi, zarówno własnej, jak i kolegów z pracy. Większość uważała ją za drobne dziwactwo albo pretekst nieśmiałego mądrali do nawiązywania rozmów. To prawda, ale przede wszystkim pomagała mi rozładować podenerwowanie. Uspokajała mnie.

Kupiłem kilka kostek i rozdałem je. Każdemu, kto otrzymał prezent, udzielałem wskazówek. Im bardziej wszyscy przywykli do widoku własnej kostki, tym mniejszą odczuwali potrzebę, by przyglądać się mojej.

Udawało mi się utrzymywać serdeczne kontakty ze strażnikami, a przynajmniej tak sobie wmawiałem, w dużej mierze dlatego że wiedziałem, gdzie są myślami: gdzieś indziej. Wykonywałem kiedyś podobną pracę w Ośrodku Zaawansowanych Badań Językowych. Wiedziałem, jakie to nużące zajęcie – stać całą noc na nogach, udając czujność. Bolą cię stopy. Po pewnym czasie boli cię wszystko. I doskwiera ci taka samotność, że masz ochotę rozmawiać ze ścianą.

Postanowiłem, że będę zabawniejszy niż ściana i na potrzeby każdej ludzkiej przeszkody w postaci ochroniarza opracowałem stosowną gadkę. Z jednym strażnikiem rozmawiałem o bezsenności i trudności z odsypianiem w dzień (pamiętaj, że pracowałem na nocnej zmianie, więc toczyliśmy te rozmowy około drugiej nad ranem). Z innym dyskutowałem na tematy polityczne. Nazywał demokratów „demoszmatami”, więc przygotowywałem się, czytając skrajnie prawicowy serwis Breitbart News. Wszyscy mieli jedną wspólną cechę: uśmiechali się na widok mojej kostki. Kiedy pracowałem w Tunelu, od prawie wszystkich strażników usłyszałem mniej więcej: „Jezu, pamiętam, jak się taką bawiłem, kiedy byłem mały”, a następnie za każdym razem: „Próbowałem zdzierać naklejki, żeby dopasować kolory”, „Ja też, stary. Ja też”.

Udawało mi się odprężyć – ale tylko trochę – dopiero wówczas, kiedy znalazłem się już w domu. Niepokoiło mnie, że nasze mieszkanie mogło być na podsłuchu; to kolejna z listy urzekających metod, które FBI stosowało wobec osób podejrzewanych o niedostateczną lojalność. Zbywałem Lindsay zawsze, gdy wyrażała obawy z powodu mojego niedoboru snu – aż w końcu znienawidziła mnie za to, a ja znienawidziłem siebie. Ona szła do łóżka, ja na kanapę, gdzie jak dziecko chowałem się z laptopem pod kocem, ponieważ bawełna neutralizuje kamery. Kiedy przestało mi bezpośrednio zagrażać aresztowanie, znalazłem siłę, by skoncentrować się na przenoszeniu plików na większy zewnętrzny nośnik pamięci za pośrednictwem mojego laptopa – tylko ktoś, kto bardzo słabo rozumie technologię, mógłby pomyśleć, że zachowam dane na laptopie na zawsze – i zabezpieczaniu ich wieloma warstwami algorytmów kryptograficznych wykorzystujących różne metody. Dzięki temu dane miały pozostać chronione, nawet gdyby ktoś złamał jeden z poziomów szyfrowania.

Dołożyłem starań, by nie zostawić po sobie śladów w pracy oraz po szyfrowaniu usunąć wszystkie pozostałości plików z domu. Wiedziałem jednak, że dokumenty naprowadzą agencję na mój trop, kiedy wyślę je dziennikarzom i zostaną odszyfrowane. Śledczemu przygotowującemu listę pracowników, którzy uzyskali albo mogli uzyskać dostęp do wszystkich tych materiałów, najprawdopodobniej pozostałoby wymienić tylko jedno nazwisko: moje. Mogłem dostarczyć reporterom mniej dokumentów, ale wpłynęłoby to na skuteczność ich działań. Ostatecznie pogodziłem się z faktem, że nawet pojedynczy slajd z prezentacji czy też plik PDF narażał mnie, ponieważ wszystkie pliki zawierają metadane, niewidzialne znaczniki, na których podstawie można określić ich pochodzenie.

Nie potrafiłem wymyślić, jak rozwiązać kwestię metadanych. Niepokoiłem się z jednej strony, że jeśli nie wymażę informacji umożliwiających ustalenie mojej tożsamości, wypłynie ona na jaw z chwilą, gdy dziennikarze rozszyfrują i otworzą pliki, a z drugiej strony bałem się, że wymazując te wskazówki bardzo starannie, będę ryzykował dokonanie w plikach zmian, które mogłyby podważyć ich autentyczność. Co było ważniejsze: osobiste bezpieczeństwo czy dobro społeczeństwa? Może się wydawać, że to łatwy wybór, ale potrzebowałem dłuższego czasu, by zdecydować, że wezmę ryzyko na siebie i pozostawię metadane bez zmian.

Poniekąd przekonał mnie strach, że nawet jeśli usunę metadane, o których istnieniu wiedziałem, w plikach mogą znajdować się inne cyfrowe znaki wodne, których nie znałem i nie potrafiłem wyszukać. Kolejnym powodem była trudność, jakiej nastręcza oczyszczanie dokumentów dla pojedynczego użytkownika. Dokument taki jest oznaczony specjalnym kodem sprawiającym, że kiedy redakcja prasowa prosi rząd o potwierdzenie autentyczności pliku, rząd wie, kto go wypuścił. W niektórych wypadkach niepowtarzalny identyfikator był ukryty w kodzie daty albo sygnatury czasowej, w innych zawierał się w układzie pikseli grafiki albo loga. Istniała jednak możliwość, że tkwił zakamuflowany w nieznanym mi miejscu albo w sposób, który w ogóle nie przyszedł mi do głowy. Ten aspekt powinien mnie zniechęcić, ale w praktyce dodał mi odwagi. Przeszkoda technologiczna zmusiła mnie, bym zmierzył się z koniecznością odrzucenia anonimowości, którą praktykowałem całe życie, i ujawnił się jako źródło przecieków. Postanowiłem, że będę bronił moich zasad, podpisując się pod nimi własnym nazwiskiem i skazując się tym samym na potępienie.

Wszystkie wybrane przeze mnie dokumenty mieściły się na jednej pamięci USB, którą zostawiłem na blacie biurka w domu. Wiedziałem, że

dane są tam równie bezpieczne, co w macierzystej placówce. W gruncie rzeczy nawet bardziej, bo zostały wielopoziomowo zaszyfrowane różnymi metodami. Na tym polega niepowtarzalna magia sztuki kryptograficznej – odrobina matematyki może zdziałać więcej niż wszystkie karabiny i drut kolczasty: pozwala zachować tajemnicę.

24_Zaszyfruj|

Większość osób używających komputerów, w tym przedstawiciele czwartej władzy, sądzi, że poza upoważnieniami do odczytu, zapisu i uruchamiania plików istnieje czwarte: do ich usuwania.

Możliwość usuwania plików przez użytkownika jest wszechobecna. Pojawia się w warstwie sprzętowej jako klawisz na klawiaturze oraz w warstwie oprogramowania jako opcja, którą można wybrać z rozwijanego menu. Z wciśnięciem klawisza „delete” albo „backspace”, bądź wybraniem opcji „Usuń” wiążą się swego rodzaju ostateczność i poczucie odpowiedzialności. Czasami nawet pojawia się okienko z prośbą o potwierdzenie: „Jesteś pewien?”. Skoro komputer ci nie ufa i wymaga zapewnienia – kliknięcia „Tak” – wydaje się logiczne, że operacja usunięcia niesie za sobą konsekwencje, być może nawet nieodwracalne.

I tak niewątpliwie jest w rzeczywistości pozakomputerowej, gdzie ludzie od zawsze dysponowali potężnymi możliwościami usuwania różnych rzeczy. Mimo to wiele jest przykładów despotów z całego świata, którzy odkryli poniewczasie, że nie wystarczy po prostu zniszczyć wszystkich kopii dokumentu, by się tego dokumentu naprawdę pozbyć. Trzeba również usunąć wszelką pamięć o nim – mam tu na myśli konieczność pozbycia się wszystkich ludzi, którzy pamiętają jego treść, jak również wszystkich innych dokumentów, które o nim wspominają, oraz osób, które pamiętają te inne dokumenty. Dopiero wtedy być może – ale tylko być może – przekaz przestaje istnieć.

Funkcja usuwania pojawiła się już w najwcześniejszych komputerach cyfrowych. Ich projektanci rozumieli, że w świecie oferującym nieskończoną liczbę opcji niektóre wybory w nieunikniony sposób okażą się błędne. Użytkownicy niezależnie od tego, czy dysponowali rzeczywistą kontrolą nad maszyną na poziomie technicznym, czy nie, musieli mieć poczucie, że tak jest, przede wszystkim w odniesieniu do wszystkiego, co sami tworzyli. Skoro mogli zakładać pliki, powinni również – bez żadnych ograniczeń – móc je „odzałożyć”. Możliwość niszczenia rzeczy, które się stworzyło, i rozpoczynania od nowa była podstawową funkcjonalnością dającą użytkownikowi wrażenie panowania nad sytuacją bez względu na to, że w praktyce mógł być uzależniony od chronionego patentami sprzętu, którego nie potrafił naprawić, i oprogramowania, którego nie wolno mu było modyfikować, oraz spętany przepisami platformy zarządzanej przez stronę trzecią.

Zastanów się, dlaczego sam wybierasz komendę „Usuń”. Używając komputera osobistego, robisz to prawdopodobnie dlatego, że chcesz pozbyć się jakiegoś dokumentu, bo coś poszło nie tak, lub pobranego pliku, ponieważ już go nie potrzebujesz… lub wolałbyś, żeby nikt się nie dowiedział, iż był ci potrzebny. Do usunięcia z konta e-mailowego może się kwalifikować wiadomość od dawnej kochanki, której nie chcesz pamiętać albo nie chcesz ujawniać swojej obecnej partnerce, czy też potwierdzenie udziału w proteście, na który rzeczywiście się wybrałeś. Jeśli zaś chodzi o smartfona, to możesz chcieć usunąć historię odwiedzonych miejsc albo niektóre ze zdjęć, filmów i osobistych wiadomości automatycznie wgranych do chmury.

W każdym z tych wypadków wydaje się, że po usunięciu plik przestaje istnieć.

W rzeczywistości jednak usuwanie nigdy nie funkcjonowało pod względem technicznym tak, jak to sobie zwykle wyobrażamy. Opcja oferowana przez urządzenia komputerowe jest wytworem wyobraźni, powszechną fikcją, kłamstwem z niezbyt szlachetnych pobudek, którego celem jest uspokoić cię i dać poczucie, że wszystko jest w porządku. Usunięty plik znika z widoku, ale z informatycznego punktu widzenia „usuwanie” jest po prostu formą „zapisu”. Zazwyczaj kiedy wybierasz opcję „Usuń” albo wciskasz klawisz „delete” po zaznaczeniu jednego ze swoich plików, zawarte w nim dane – przechowywane gdzieś głęboko na dysku – pozostają nietknięte. Konstrukcja wydajnych nowoczesnych systemów operacyjnych nie pozwala im grzebać głęboko w trzewiach nośników danych wyłącznie po to, by coś wymazać. Zadowalają się dodaniem do mapy, która podpowiada komputerowi, gdzie znajdują się poszczególne dokumenty – tak zwanej tablicy plików – adnotacji o treści: „Nie wykorzystuję tego miejsca do niczego ważnego”. Oznacza to, że podobnie jak zapomniana książka w ogromnej bibliotece twój pozornie wymazany plik może zostać odczytany przez osobę, której będzie się chciało wysilić, żeby go odszukać. Usunięcie wpisu z bibliotecznego katalogu nie powoduje, że książka znika z półki.

Co ciekawe, możesz się o tym łatwo przekonać. Kiedy następnym razem będziesz kopiował jakiś plik, zadaj sobie pytanie, dlaczego trwa to tak długo w porównaniu z następującym natychmiast usunięciem. Otóż dlatego, że usunięcie pliku w praktyce tylko maskuje jego istnienie. Komputerów, mówiąc krótko, nie projektuje się tak, by naprawiały błędy, lecz je ukrywały – i to wyłącznie przed tymi, którzy nie wiedzą, gdzie ich szukać.

Ostatnie dni 2012 roku przyniosły ponure wieści: dwa spośród najważniejszych krajów wchodzących w skład Sojuszu Pięciorga Oczu

zamierzały rozmontować jedne z ostatnich ustawowych zabezpieczeń przed powszechną inwigilacją. Rządy Australii i Wielkiej Brytanii proponowały nowe prawo, które nakładało na dostawców usług obowiązek gromadzenia metadanych telefonicznych i internetowych. Był to pierwszy taki wypadek: w teorii demokratyczna władza otwarcie wyraziła chęć ustanowienia swego rodzaju wywiadowczej machiny czasu umożliwiającej rządzącym przeglądanie wydarzeń z życia dowolnej osoby na przestrzeni minionych miesięcy albo nawet lat. Próby te stanowiły niezaprzeczalny znak, w każdym razie moim zdaniem, że tak zwany świat zachodni przeistoczył się z twórcy i obrońcy wolnego internetu we wroga i przyszłego niszczyciela sieci. Choć ustawy, o których mowa, próbowano uzasadniać koniecznością ochrony społeczeństwa, groziły one tak daleko idącym naruszeniem codziennej prywatności niewinnych, że przeraziły – bardzo słusznie – nawet mieszkańców innych krajów uważających, że ich ta sprawa nie dotyczy (być może dlatego, że ich rządy inwigilowały obywateli w tajemnicy).

Te publiczne działania na rzecz masowej inwigilacji dowiodły raz na zawsze, że nie ma najmniejszych szans na naturalny sojusz technologii i władzy. Rozłam pomiędzy dwiema zaskakująco przeplatającymi się społecznościami, do których należałem – amerykańskiego wywiadu i globalnego plemienia specjalistów z dziedziny technologii komputerowej – nabrał definitywnego charakteru. Na samym początku mojej kariery w służbach wywiadowczych udawało mi się godzić te dwie kultury. Płynnie przechodziłem od obowiązków szpiega do relacji z najróżniejszymi cywilami zajmującymi się tematem prywatności internetowej – od hakerów-anarchistów po stateczniejszych intelektualistów działających w Torze, którzy przekazywali mi najnowsze wieści ze świata akademickiej informatyki i kształtowali moje poglądy polityczne. Przez

całe lata dawałem radę wmawiać samemu sobie, że jesteśmy w zasadzie po tej samej stronie historii: wszyscy staramy się chronić internet, utrzymywać w nim wolność słowa i wolność od strachu. Straciłem jednak zdolność podtrzymywania tego urojenia. Rząd – mój pracodawca – jednoznacznie stał się wrogiem. Ja zaś niedawno przekonałem się o tym, co zawsze podejrzewali moi koledzy informatycy. Nie mogłem im jednak o tym powiedzieć. Jeszcze nie teraz.

Mogłem jednak zrobić coś innego – mianowicie pomóc w takim stopniu, by nie zagroziło to moim planom. I tak oto znalazłem się w Honolulu, pięknym mieście, które wcześniej nie stanowiło obszaru moich zainteresowań, w roli jednego z gospodarzy i prelegentów na CryptoParty. Była to nowa forma spotkań aktywistów z międzynarodowego społecznego ruchu kryptologicznego; tu informatycy dzielili się swoim czasem i wiedzą, prowadząc darmowe ogólnodostępne zajęcia o tematyce związanej z cyfrową samoobroną, czyli ochroną internetowej komunikacji. Pod wieloma względami warsztaty pokrywały się z tym, czego uczyłem w JCITA, więc chętnie skorzystałem z okazji, by wziąć w nich udział.

Możesz odnieść wrażenie, że było to bardzo ryzykowne z mojej strony, zważywszy na wszystko, czym się wówczas zajmowałem; wolałbym jednak moją decyzję postrzegać jako dowód ogromnej wiary w metody szyfrowania, których uczyłem – te same, którymi zabezpieczyłem znajdujący się w moim mieszkaniu nośnik pełen danych o nadużyciach agencji – i których nie była w stanie obejść nawet NSA. Zdawałem sobie sprawę, że ani dokumenty, ani nakład pracy dziennikarzy nie wystarczą, by w pełni odnieść się do zagrożenia czyhającego na świat. Ludzie potrzebowali narzędzi, dzięki którym mogliby się bronić, i wiedzy, jak z nich korzystać. Z racji zaś tego, że w najbliższym czasie miałem przekazać te narzędzia dziennikarzom, zacząłem się niepokoić, że

podchodzę do sprawy zbyt technicznie. Miałem za sobą wiele godzin szkolenia kolegów z pracy, więc uznałem, że pomysł, by ująć temat tak, by dopasować go do poziomu niewykwalifikowanej widowni, będzie z korzyścią i dla mnie, i dla pozostałych. Poza tym autentycznie tęskniłem do nauczania: minął rok, odkąd ostatni raz stałem naprzeciw uczniów, a kiedy tylko znalazłem się z powrotem w tej roli, zdałem sobie sprawę, że uczyłem czegoś wartościowego, ale nie te osoby, które powinienem.

Pisząc o swoich uczniach, nie mam na myśli zorganizowanej grupy, z jaką pracowałem w szkole wywiadowczej albo w agencyjnych salach odpraw. CryptoParty odbywało się w jednej sali galerii sztuki mieszczącej się za sklepem z meblami i przestrzenią coworkingową. Gdy ustawiałem rzutnik, którym zamierzałem wyświetlać slajdy tłumaczące, jak łatwo jest prowadzić serwer Tora, by pomóc – na przykład – mieszkańcom Iranu, ale również Australii, Wielkiej Brytanii i Stanów, do sali napływali moi uczniowie – zróżnicowana grupa złożona z obcych mi osób oraz kilku nowych znajomych, z którymi dotychczas rozmawiałem wyłącznie przez internet. Łącznie, jak sądzę, tamtego grudniowego wieczora pojawiło się może dwadzieścia osób, by uczyć się ode mnie i współprelegentki Runy Sandvik, bystrej młodej Norweżki z zespołu tworzącego projekt Tor. (Runa później została dyrektorką do spraw bezpieczeństwa informacji w redakcji „New York Timesa”; dziennik ten sponsorował kolejne edycje organizowanych przez nią CryptoParty). Naszych słuchaczy nie łączyło zainteresowanie Torem, ani nawet strach przed inwigilacją, lecz pragnienie odzyskania poczucia kontroli nad prywatnymi obszarami życia. Wśród zebranych znaleźli się: kilka starszych osób z ulicy, miejscowy dziennikarz zajmujący się tematem hawajskiego ruchu Occupy! i kobieta, której były partner z zemsty rozprowadził w sieci materiały porno z jej udziałem. Zaprosiłem też niektórych kolegów z pracy w nadziei, że zainteresuję ich

tym ruchem; chciałem też pokazać, że nie próbuję ukrywać przed agencją swojego zaangażowania. Pojawił się jednak tylko jeden służbowy znajomy i przez całe spotkanie siedział w ostatnim rzędzie z szeroko rozstawionymi nogami, rękami złożonymi na piersi i aroganckim uśmieszkiem na twarzy.

Rozpocząłem prezentację od omówienia iluzorycznego charakteru operacji wymazywania plików, której cel, czyli całkowite usunięcie, jest niemożliwy do osiągnięcia. Słuchacze natychmiast to pojęli. Następnie wyjaśniłem, że w najlepszym razie dane, których nie chcieli nikomu pokazywać, można było nadpisać: zabazgrać, można powiedzieć, losowymi albo pseudolosowymi danymi tak mocno, że pierwotna informacja stawała się nieczytelna. Jednak nawet to rozwiązanie, ostrzegłem, ma wady. Istniało pewne prawdopodobieństwo, że system operacyjny komputera po cichu ukrył kopię pliku, który pragnęli usunąć, w jakimś miejscu tymczasowego przechowywania, gdzie użytkownik nie ma dostępu.

I przeszedłem do tematu szyfrowania.

Usunięty plik to marzenie inwigilującego i koszmar dla osoby inwigilowanej, ale szyfrowanie jest, a przynajmniej powinno być czymś zupełnie powszednim. Stanowi jedyną autentyczną ochronę przed szpiegowaniem. Kiedy zaszyfrujesz cały dysk, twoi wrogowie nie będą w stanie przekopać go w poszukiwaniu usuniętych plików ani niczego innego – chyba że posiadają twój klucz szyfrujący. Jeśli wszystkie e-maile w twojej skrzynce odbiorczej są zaszyfrowane, Google nie może stworzyć twojego profilu na ich postawie – chyba że posiada twój klucz szyfrujący. Jeśli cała zawartość twojej komunikacji przepływającej przez wrogie australijskie, brytyjskie, amerykańskie, chińskie albo rosyjskie sieci jest zaszyfrowana, szpiedzy nie mogą jej czytać – chyba że dysponują twoim kluczem szyfrującym. Na tym polega hierarchia społeczna w świecie kryptografii: cała władza leży w rękach tego, kto posiada klucz.

Szyfrowanie opiera się, jak już tłumaczyłem, na algorytmach. „Algorytm szyfrujący” brzmi groźnie i na pewno onieśmiela, kiedy wypisze się go na kartce albo tablicy, jednak sama koncepcja jest dość banalna. Szyfrowanie to matematyczna metoda odwracalnego przekształcania informacji – takich jak twoje e-maile, rozmowy telefoniczne, zdjęcia, filmy i pliki – w taki sposób, że stają się niezrozumiałe dla każdego, kto nie posiada kopii klucza szyfrującego. Możesz sobie wyobrazić nowoczesny algorytm szyfrujący jako magiczną różdżkę, jednym machnięciem tłumaczącą każdą literę dokumentu na język zrozumiały tylko dla ciebie i dla tych, którym ufasz, a klucz jako wyjątkowe magiczne słowa wypowiadane w formie zaklęcia uwalniającego moc różdżki. Nie ma znaczenia, jak wiele osób wie, że użyłeś różdżki, pod warunkiem, że ci, którym nie ufasz, nie znają twoich osobistych magicznych słów.

Pod względem technicznym algorytmy szyfrujące to tylko zestawy zadań matematycznych wymyślonych w taki sposób, by ich rozwiązanie było niewiarygodnie trudne nawet dla komputerów. Klucz jest jedyną wskazówką; na jej podstawie możliwe staje się znalezienie wyniku. Wprowadzasz swoje dane w użytecznej formie, czyli tak zwany tekst jawny, do algorytmu, który wypluwa niezrozumiały bełkot zwany szyfrogramem. Każdy, kto chce odczytać twój szyfrogram, wprowadza go z powrotem do algorytmu w towarzystwie – co bardzo ważne – poprawnego klucza i otrzymuje na powrót tekst jawny. Różne algorytmy zapewniają różne stopnie bezpieczeństwa, jednak moc klucza często wynika z jego długości, od której zależy stopień skomplikowania obliczeń wymaganych do rozwiązana zadania matematycznego leżącego u podstaw algorytmu. W algorytmach, w których dłuższy klucz przekłada się na lepsze zabezpieczenie, wzrost bezpieczeństwa ma charakter wykładniczy. Jeśli założyć, że inwigilator potrzebuje jednego dnia, by złamać klucz 64-

bitowy – który miesza twoje dane w jeden z 2^{64} możliwych sposobów (co oznacza 18 446 744 073 709 551 616 niepowtarzalnych permutacji) – złamanie klucza 65-bitowego zajmie mu dwukrotnie więcej czasu, czyli dwa dni, a 66-bitowego – cztery. Złamanie 128-bitowego klucza wymagałoby okresu 2^{64} razy dłuższego niż dzień, czyli pięćdziesięciu biliardów lat. Do tego czasu być może nawet zostanę ułaskawiony.

Do porozumiewania się z dziennikarzami wykorzystałem klucze 4096- i 8192-bitowe. Oznaczało to, że jeśli nie dokona się kolejna rewolucja technologiczna lub nie zajdą fundamentalne zmiany zasad rządzących rozkładem liczb na czynniki, NSA nie odczyta zawartości mojego dysku, choćby oddelegowała do tego wszystkich swoich kryptoanalityków i udostępniła im całą moc obliczeniową świata.

Dlatego właśnie szyfrowanie jest najlepszym narzędziem w walce z każdą inwigilacją. Gdyby wszystkie nasze dane, w tym nasze rozmowy i wiadomości, były cyfrowo zaszyfrowane przez całą drogę od nadawcy do odbiorcy, żaden rząd – ani żadna instytucja, która mogłaby powstać w świecie ograniczonym znanymi nam prawami fizyki – nie byłyby zdolne ich odczytać. Rządzący wciąż mogliby przechwytywać i gromadzić naszą łączność, ale miałaby ona z jego perspektywy postać zwykłego szumu. Szyfrowanie rozmów i wiadomości praktycznie wymazałoby je z pamięci wszystkich podmiotów, z którymi utrzymujemy relacje. Z praktycznego punktu widzenia cofnęłoby zgodę na inwigilację tym, którym w gruncie rzeczy nigdy jej nie udzieliliśmy.

Jeśli rząd pragnie uzyskać dostęp do zaszyfrowanych rozmów i wiadomości, ma tylko dwie możliwości: zdobyć klucze albo kontrolę nad ich posiadaczami. Może organizować ataki na punkty końcowe łączności, czyli sprzęt i oprogramowanie dokonujące szyfrowania, lub wywierać nacisk na producentów urządzeń, by intencjonalnie sprzedawali produkty,

które zaszyfrują dane w niewłaściwy sposób. Może również zwodzić międzynarodowe organizacje normalizacyjne, by doprowadzić do przyjęcia wadliwych algorytmów szyfrujących posiadających „tylne drzwi”, czyli tajne możliwości dostępu do danych. Inna możliwość to wykorzystanie podatności na ataki, której rząd sam nie stworzył, lecz jedynie odkrył, i zhakowanie tą metodą twojego komputera i wykradzenie kluczy – pionierami tej techniki byli kryminaliści, lecz dziś stosowana jest z lubością przez najważniejsze kraje świata, mimo że wymaga umyślnego niełatania ogromnych dziur w cyberzabezpieczeniach kluczowych elementów globalnej infrastruktury.

Najlepiej zachować bezpieczeństwo naszych kluczy dzięki tak zwanym protokołom wiedzy zerowej, czyli metodzie, która daje pewność, że wszelkie dane przechowywane na nośnikach zewnętrznych – na przykład w firmowej chmurze – są zaszyfrowane algorytmem wykonywanym na twojej maszynie przed wgraniem pliku do sieci, a klucz nie jest nigdzie udostępniany. W protokołach wiedzy zerowej klucze znajdują się wyłącznie w rękach użytkownika i niczyich innych. Nie mają do nich dostępu żadna agencja, firma ani wróg.

W dbałości o bezpieczeństwo klucza, którym zakodowałem tajemnice NSA, poszedłem o krok dalej: skonstruowałem go z wielu innych kluczy wiedzy zerowej.

Możesz wyobrazić to sobie następująco: powiedzmy, że po zakończeniu mojego wykładu na CryptoParty stanąłem przy wyjściu i za każdym razem, gdy mijał mnie jeden z dwudziestu członków widowni, by rozpłynąć się w honolulskiej nocy, szeptałem mu do ucha słowo – jedno słowo, którego nie słyszał nikt inny i które wolno mu było powtórzyć dopiero wówczas, jeśli kiedyś znajdziemy się wszyscy w tym samym pomieszczeniu. Tylko ściągając całą dwudziestkę i każąc im powtórzyć słowa w tej samej

kolejności, w jakiej pierwotnie je rozdysponowałem, dało się odtworzyć całe dwudziestowyrazowe zaklęcie. Gdyby choć jedna osoba zapomniała swojego słowa albo zebrani wyrecytowaliby je w kolejności odbiegającej w jakikolwiek sposób od początkowej, zaklęcie nie zadziałałoby i nie przywołałoby magii.

Moje klucze do dysku zawierającego wykradzione dokumenty były zorganizowane podobnie, ale z jednym wyjątkiem: choć rozsiałem większość sylab zaklęcia, zostawiłem jedną dla siebie. Pochowałem fragmenty inkantacji w najróżniejszych miejscach, ale wystarczyło, bym zniszczył tę jedną, którą nosiłem przy sobie, by na zawsze uniemożliwić wszelki dostęp do tajemnic NSA.

25_Chłopiec|

Dopiero z perspektywy czasu mogę ocenić, jak daleko zaszedłem. Z ucznia, który nie potrafił odezwać się na forum klasy, zmieniłem się w nauczyciela języka nowej ery, z syna skromnych rodziców należących do klasy średniej i zatrudnionych na państwowych posadach w wyspiarza zarabiającego tak dobrze, że pieniądze przestały mieć dla mnie znaczenie. W ciągu zaledwie siedmiu lat kariery zawodowej wspiąłem się ze stanowiska komputerowca obsługującego lokalne serwery na pozycję tworzącego i wdrażającego globalne systemy – od nocnego stróża do mistrza w swoim zawodzie w Pałacu Tajemnic, jak zwano NSA.

Zbyt szybki awans nawet najlepiej wykwalifikowanej osoby stwarza jednak spore ryzyko potencjalnych problemów – ma ona za mało czasu, by wyzbyć się idealizmu i przyjąć cyniczne podejście. Moja funkcja w służbach wywiadowczych zapewniała mi zaskakująco szeroką wiedzę. Choć znajdowała się na dole kierowniczej drabiny, to jeśli chodzi o dostęp do informacji, sięgałem szczytu. Dawało mi to wprawdzie niezwykłą i – prawdę mówiąc – niezasłużoną możliwość oglądu wywiadu w całej jego ponurej okazałości, ale też jeszcze bardziej podsycało ciekawość związaną z pewną kwestią, która stale mi umykała: jaka jest absolutna granica metod inwigilacyjnych agencji. I nie chodziło tu o granicę związaną z polityką lub prawem, lecz raczej z bezwzględnymi, nieustępliwymi możliwościami machiny, która, o czym już wiedziałem, obejmowała zasięgiem cały świat. Czy istnieje ktoś, kogo ta machina nie jest w stanie inwigilować? Czy są miejsca, gdzie nie może dotrzeć?

Jedynym sposobem, żeby się tego dowiedzieć, było zejście niżej, porzucenie dającego pełny obraz punktu obserwacyjnego dla stanowiska operacyjnego z węższą perspektywą. W NSA najswobodniejszy dostęp do najsurowszej formy informacji wywiadowczych mają operatorzy wpisujący do komputerów imiona i nazwiska osób uznanych za podejrzane, zarówno Amerykanów, jak i obcokrajowców. Kiedy już tacy ludzie wpadną w tryby systemu ścisłej inwigilacji, agencji zależy, żeby dowiedzieć się wszystkiego o nich i ich komunikacji. Wiedziałem już, że moim ostatecznym celem jest właśnie ten punkt styku – miejsce, gdzie państwo przygląda się człowiekowi, a ten nie ma o tym pojęcia.

Program, który umożliwiał tak dokładną inwigilację, zwano XKEYSCORE. Najłatwiej zrozumieć jego działanie przez analogię do przeglądarki, za której pomocą analityk może przeszukiwać wszystkie zapisy twojego życia. Wyobraź sobie, że wyszukiwarka w rodzaju Google’a zamiast pokazywać strony publicznego internetu, wyświetla rezultaty pochodzące z twoich prywatnych e-maili, czatów, osobistych plików – słowem wszystko, co robiłeś w sieci. Przeczytałem sporo o tym programie, ale jeszcze go nie używałem, i teraz uświadomiłem sobie, że muszę dowiedzieć się więcej. Zająłem się XKEYSCORE’em, bo chciałem przekonać się na własne oczy, jak głęboko inwigilacja NSA wdziera się w prywatne życie – zależało mi na wiedzy, jakiej nie może dać żadna dokumentacja, a wyłącznie osobiste doświadczenie.

Jednym z nielicznych biur na Hawajach mających nieskrępowany dostęp do XKEYSCORE’a było National Threat Operations Center (NTOC, Centrum Operacyjne do spraw Zagrożeń Bezpieczeństwa Narodowego). Siedziba mieściła się w nowoczesnym, lecz bezdusznym biurowcu z pomieszczeniami urządzonymi na otwartym planie. NSA nadała mu oficjalną nazwę Rochefort Building dla uczczenia Josepha Rocheforta,

legendarnego kryptologa z czasów drugiej wojny światowej, który złamał japońskie szyfry. Większość pracowników zaczęła jednak nazywać go Roach Fort, a nawet Roach (karaluch). Kiedy złożyłem tam podanie o pracę, część obiektu była jeszcze w budowie, co od razu przypomniało mi moje pierwsze stanowisko wymagające poświadczenia bezpieczeństwa – w Ośrodku Zaawansowanych Badań Językowych. Najwyraźniej moim przeznaczeniem było zacząć i skończyć współpracę z wywiadem w niedokończonych budynkach.

NSA przeniosła do Rochefort niemal wszystkich pracujących na Hawajach tłumaczy i analityków, a także miejscowy oddział Tailored Access Operations (TAO, Operacje Specjalnego Dostępu). Była to jednostka agencji odpowiedzialna za zdalne włamywanie się do komputerów osób, które analitycy wybrali na cele – odpowiednik dawnych zespołów włamywaczy, które w domach wroga podkładali pluskwy i szukały kompromitujących materiałów. Głównym zadaniem NTOC było natomiast monitorowanie i zakłócanie działania zagranicznych odpowiedników TAO. Szczęśliwie dla moich planów okazało się, że NTOC ma wolne stanowisko o eufemistycznym tytule „analityka infrastruktury" dla podwykonawcy zatrudnionego w firmie Booz Allen Hamilton. Praca miała polegać na korzystaniu ze wszystkich narzędzi masowej inwigilacji NSA, łącznie z XKEYSCORE'a, do monitorowania aktywności w interesującej agencję „infrastrukturze", czyli internecie.

W Boozie na nowej posadzie miałem zarabiać nieco więcej, około 120 000 dolarów rocznie, ale traktowałem ją jako obniżenie statusu, pierwsze z wielu, które miały mnie czekać, gdy nieodwołalnie rozpocząłem wytracanie wysokości, pozbywając się dostępu, poświadczeń bezpieczeństwa i przywilejów w agencji. Byłem inżynierem, który stał się analitykiem, a ten ostatecznie miał stać się wygnańcem namierzanym przez

te same technologie, jakimi kiedyś zarządzał. Z tej perspektywy ta konkretna degradacja wydawała się niewielka. Właściwie z tej perspektywy wszystko wydawało się mało ważne, skoro trajektoria mojej egzystencji kierowała się z powrotem ku ziemi, coraz szybciej zbliżając się do punktu zderzenia, który będzie końcem mojej kariery, związku, wolności, a być może i życia.

Postanowiłem wywieźć swoje archiwa z kraju i przekazać je dziennikarzom, z którymi się kontaktowałem, ale zanim jeszcze zdążyłem zacząć planować, jak to wszystko rozwiązać logistycznie, musiałem wyjechać i uścisnąć kilka dłoni. Poleciałem na wschód do Waszyngtonu i przez kilka tygodni spotykałem się z nowymi szefami i kolegami; tak bardzo liczyli, że moje doskonałe rozumienie anonimizacji online pomoże im zdemaskować bardziej przebiegłe cele. Przy okazji tej podróży mogłem po raz ostatni odwiedzić dom rodzinny; wróciłem też tam, gdzie po raz pierwszy zetknąłem się z instytucją, która utraciła panowanie nad sobą, czyli do Fortu Meade. Tym razem przybywałem tam jako wtajemniczony.

W roku, kiedy osiągnąłem pełnoletność, nieco ponad dziesięć burzliwych lat wcześniej, jeden dzień odcisnął się piętnem i całkowicie zmienił nie tylko ludzi pracujących w centrali NSA, ale również samo miejsce. Po raz pierwszy dostrzegłem to wtedy, gdy zatrzymano mnie w wynajętym samochodzie podczas zjazdu z Canine Road na parking agencji, który w mojej pamięci nadal kojarzył mi się z paniką, dzwoniącymi telefonami, jazgotem klaksonów i wyciem syren. Od 11 września 2001 roku wszystkie drogi prowadzące do centrali NSA były na stałe zamknięte i wjechać tam mogły wyłącznie osoby ze specjalnymi identyfikatorami służb wywiadowczych; jeden z nich miałem wówczas na szyi.

Czas wolny od wylewnych powitań z kierownictwem NTOC w centrali poświęcałem na uczenie się wszystkiego, czego tylko mogłem. Pracowałem na rozmaitych stanowiskach z analitykami obsługującymi różne programy i zajmującymi się różnymi celami po to, by po powrocie na Hawaje nauczyć swoich kolegów, jak korzystać z najnowszych narzędzi agencji. Tak przynajmniej brzmiało oficjalne uzasadnienie dla mojej ciekawości, która jak zawsze wybiegała dalece poza formalne wymagania i była mile widziana przez osoby o zacięciu technicznym. One z kolei jak zawsze entuzjastycznie demonstrowały mi pełne możliwości systemu, który opracowały, nie wyrażając najmniejszych wątpliwości moralnych na temat tego, do czego owe możliwości są wykorzystywane. Podczas pobytu w centrali przeszedłem też kilka testów prawidłowego korzystania z systemu, które jednak miały niewiele wspólnego z konstruktywnym szkoleniem, natomiast wiele ze zgodnością z przepisami i zabezpieczeniami proceduralnymi. Do testów można było podchodzić aż do skutku, w związku z czym inni analitycy doradzili mi, żebym dał sobie spokój z nauką reguł: „Po prostu klikaj w odpowiedzi, aż zdasz”.

W dokumentach, które później przekazałem dziennikarzom, NSA opisuje XKEYSCORE jako narzędzie o „najszerszym zasięgu”, wykorzystywane do przeszukiwania „niemal wszystkiego, co użytkownik robi w internecie”. Ze specyfikacji technicznych dowiedziałem się bardziej szczegółowo, jak się tego dokonuje – przez „pakietyzację” i „podziały na sesje”, czyli rozdzielanie danych z sesji użytkownika online na pakiety nadające się do analizy – ale żadna posiadana wiedza nie przygotowała mnie na widok systemu w działaniu.

Krótko mówiąc: spośród wszystkich rzeczy ze świata nauki, jakie widziałem w życiu, ta była najbardziej zbliżona do science fiction. Oto miałem przed sobą interfejs, za którego pośrednictwem można było wpisać

adres, numer telefonu lub adres IP niemal każdej osoby fizycznej, a potem przeglądać historię jej aktywności internetowej. Czasem możliwe było nawet odtworzenie nagrania sesji online – na swoim ekranie widziałeś całą zawartość ekranu podglądanego komputera. Mogłeś przeczytać e-maile jego użytkownika, historię przeglądarki, treści zamieszczane przez niego w mediach społecznościowych, dosłownie wszystko. Można było również włączyć powiadomienia mające pojawiać się na ekranie, kiedy interesująca cię osoba lub urządzenie zaczną być aktywne w internecie. A przeglądając pakiety danych internetowych, nieraz widziało się, jak pytanie wpisywane przez użytkownika do przeglądarki ukazuje się litera po literze, bo wiele stron przesyła znak po znaku w miarę wpisywania frazy. Gdy litery i wyrazy wyświetlały się na ekranie, przypominało to obserwowanie autouzupełniania, tyle że nie kryła się za tym inteligencja sztuczna, lecz ludzka.

Jedynie podczas tygodni spędzonych w Forcie Meade i krótkiego pobytu w siedzibie Booz na Hawajach byłem bezpośrednim świadkiem popełniania nadużyć, o których wcześniej czytałem w wewnętrznych dokumentach. Dopiero widząc ten proceder, zdałem sobie sprawę, jak bardzo moje stanowisko w systemie było odizolowane od poziomu zero, czyli bezpośrednich szkód. Stopień izolacji kierownictwa agencji i – skoro już o tym mowa – prezydenta Stanów Zjednoczonych mogę sobie tylko wyobrażać.

Nie wpisywałem do XKEYSCORE’a nazwisk dyrektora agencji ani prezydenta, chociaż kiedy już dobrze zapoznałem się z działaniem systemu, uświadomiłem sobie, że mógłbym. Znajdowały się tam dane o komunikacji wszystkich – dosłownie wszystkich. Początkowo bałem się, że jeśli zacznę wyszukiwać osoby ze szczytów władzy, zostanę przyłapany i zwolniony albo spotka mnie coś jeszcze gorszego. Ale okazało się, że można

zaskakująco łatwo zamaskować sprawdzanie nawet najbardziej prominentnych osób, kodując zapytania w formie zapisu maszynowego, który będzie dla XKEYSCORE'a całkowicie zrozumiały, choć dla człowieka wyglądałby jak śmieci. Gdyby kontrolerzy odpowiedzialni za analizę wyszukiwanych haseł chcieli dokładniej przyjrzeć się temu, co robię, ujrzeliby tylko strzępy niezrozumiałego kodu, podczas gdy ja mógłbym przeglądać najbardziej osobiste strony sędziów Sądu Najwyższego lub kongresmenów.

O ile wiem, moi nowi koledzy nie zamierzali aż tak poważnie nadużywać swoich możliwości, choć gdyby nawet tak było, i tak by mi o tym nie powiedzieli. Jeśli już myśleli o niewłaściwym wykorzystywaniu systemu, to nie na gruncie zawodowym, lecz raczej osobistym. Ich sposób rozumowania doprowadził między innymi do powstania wypaczonej praktyki LOVEINT, której nazwa jest sprośną parodią terminów HUMINT i SIGINT. Polega ona na wykorzystywaniu przez analityków programów agencji do inwigilacji byłych i obecnych partnerów czy obiektów przelotnych romansów, na przykład czytania ich e-maili i podsłuchiwania rozmów telefonicznych oraz do stalkingu online. Pracownicy NSA dobrze wiedzą, że złapania na gorącym uczynku zdarzały się tylko najgłupszym analitykom. Poza tym, choć przepisy mówią, że za wykorzystywanie narzędzi inwigilacji do celów prywatnych można zostać skazanym na karę więzienia nawet do dziesięciu lat, to nikt nie spędził z tego powodu za kratami ani dnia. Analitycy doskonale zdają sobie sprawę, że organy ścigania nie wniosą przeciw nim oskarżeń, bo nie można kogoś skazać za nadużywanie systemu masowej inwigilacji, jeśli zaprzecza się jego istnieniu. Zrozumiałem, jak wyglądają oczywiste następstwa takiej polityki, kiedy siedziałem pod tylną ścianą zabezpieczonego biura V22 w centrali NSA z dwoma bardziej utalentowanymi analitykami infrastruktury, których

miejsce pracy zdobił ponad dwumetrowej wysokości plakat ze słynnym wookiem Chewbaccą z *Gwiezdnych wojen*. Kiedy jeden z nich wyjaśniał mi szczegółowo procedury bezpieczeństwa namierzanego przez niego celu, jego kolega co pewien czas obracał się na krześle i przerywał mu z uśmiechem, żeby pokazać przechwycone nagie zdjęcia, mówiąc: „Ej, zobacz tę!” – na co mój rozmówca niezmiennie odpowiadał: „Wow!” albo: „Niezła!”. Najwyraźniej była to nieformalna waluta biurowa, a niepisana zasada głosiła, że ilekroć znajdziesz nagie zdjęcia lub filmy atrakcyjnych celów – lub kogoś, kto się z nimi kontaktuje – musisz je pokazać reszcie chłopaków, przynajmniej jeśli nie ma w pobliżu żadnej kobiety. Dzięki temu wiesz, że możesz ufać każdemu koledze, wszyscy bowiem współuczestniczycie w przestępstwie.

Podczas używania XKEYSCORE’a szybko można się zorientować, że niemal wszystkie osoby na świecie korzystające z internetu mają co najmniej dwie cechy wspólne – wszystkim zdarzyło się odwiedzić strony pornograficzne oraz wszyscy przechowują zdjęcia i filmiki przedstawiające rodzinę. Ta obserwacja sprawdzała się praktycznie w każdym przypadku, niezależnie od płci, pochodzenia etnicznego, koloru skóry i wieku – od najokrutniejszych terrorystów do najsympatyczniejszych staruszków, którzy nota bene mogli być dziadkami, rodzicami lub kuzynami tych pierwszych.

I właśnie informacje dotyczące rodzin najbardziej mnie poruszały. Szczególnie utkwiło mi w pamięci pewne dziecko – chłopiec z Indonezji. Nie powinienem interesować się tym chłopczykiem, ale siłą rzeczy musiałem, bo moich pracodawców ciekawił jego ojciec. Przystąpiłem zatem do zapoznawania się ze współdzielonymi folderami dotyczącymi celu, przygotowanymi przez analityka osób, którego praca w większości polega na przeszukiwaniu zapisów czatów, skrzynek pocztowych Gmaila i wiadomości na Facebooku. Dzięki temu nie musiałem się borykać

z trudniejszymi, mniej przejrzystymi danymi pochodzącymi ze zhakowanego ruchu internetowego, dostarczanymi przez analityka infrastruktury.

Ojciec chłopca był inżynierem, tak jak mój, ale w przeciwieństwie do mojego nie pracował dla rządu ani wojska. Po prostu był naukowcem schwytanym w sieć inwigilacji. Nie pamiętam już nawet, dlaczego agencja zwróciła na niego uwagę, poza tym, że złożył podanie o pracę na uniwersytecie badawczym w Iranie. Podstawy podejrzeń często były bardzo słabo udokumentowane, jeżeli w ogóle, a powiązania niezwykle wątłe: „uważa się, że może być potencjalnie powiązany z …”, po czym następowała nazwa jakiejś organizacji międzynarodowej, mogła nią być dosłownie każda: począwszy od instytucji ustalającej standardy telekomunikacyjne przez UNICEF po jakąś rzeczywiście groźną.

Z ruchu internetowego wyodrębniono dane z komunikacji tego mężczyzny i zebrano je w folderach. Była tu kopia nieszczęsnego CV wysłanego na podejrzany uniwersytet, były jego teksty, historia przeglądarki internetowej, ostatni tydzień korespondencji przychodzącej i wychodzącej oznaczonej jego adresem IP. Miałem też przed sobą współrzędne jego geofencingu, który pomagał analitykom monitorować, czy mężczyzna nie znajduje się zbyt daleko od domu lub nie jedzie na uniwersytet na rozmowę kwalifikacyjną.

Były również rodzinne zdjęcia. I film. Siedział na nim przed swoim komputerem, tak jak ja teraz siedziałem przed moim. Tyle że na kolanach miał małe dziecko, chłopczyka w pieluszce.

Ojciec usiłował coś czytać, ale dziecko wierciło się, stukało kluczami i chichotało. Wewnętrzny mikrofon komputera zarejestrował ten śmiech, a ja słyszałem go w słuchawkach. Mężczyzna mocniej przytrzymał chłopca, a ten wyprostował się i ciemnymi rozbawionymi oczami spojrzał prosto

w kamerę. Miałem wrażenie, że patrzy bezpośrednio na mnie. Nagle uświadomiłem sobie, że wstrzymuję oddech. Zakończyłem sesję, wstałem od komputera i ze zwieszoną głową udałem się do toalety w holu, ciągnąc za sobą kabel od słuchawek, które zapomniałem zdjąć.

To dziecko i jego tata przypomnieli mi o własnym ojcu, z którym podczas krótkiego pobytu w Forcie Meade spotkałem się pewnego wieczoru na kolacji. Nie widziałem się z nim już od dłuższego czasu, ale podczas posiłku, nad sałatką Cezar i różową lemoniadą, naszła mnie nagle myśl: już nigdy więcej nie zobaczę ojca. Nie zaszkliły mi się oczy, bo bardzo mi zależało, żeby nad sobą panować, ale w środku byłem zdruzgotany. Nie mogłem mu powiedzieć o swoich zamiarach. Wiedziałem, że wezwałby gliny albo nazwał szaleńcem i postarał się zamknąć mnie w szpitalu psychiatrycznym. Zrobiłby wszystko, żeby mnie powstrzymać przed popełnieniem tego najstraszniejszego, jego zdaniem, błędu.

Mogłem tylko mieć nadzieję, że z czasem jego cierpienie zostanie złagodzone przez dumę.

Niemal wszystko, co robiłem po powrocie na Hawaje od marca do maja 2013 roku, przesycone było poczuciem, że to ostatni raz. Były to drobiazgi, ale ułatwiały mi ten okres. Znacznie mniej bolesna była myśl, że po raz ostatni w życiu zatrzymuję się w Mililani, żeby kupić curry, albo wpadam do hackerspace'u przy galerii sztuki w Honolulu lub po prostu siedzę na dachu samochodu i obserwuję spadające gwiazdy, niż dopuszczenie do siebie świadomości, że został mi tylko miesiąc z Lindsay, a potem, że już tylko przez tydzień będę obok niej spał i się budził – przez cały czas usiłując utrzymać wobec niej dystans, żeby się nie załamać.

Przygotowywałem się jak człowiek idący na śmierć. Opróżniłem rachunki bankowe, żeby rząd nie mógł zająć moich pieniędzy, a gotówkę, którą miała znaleźć Lindsay, schowałem do starej skrzynki od amunicji.

W całym domu wykonałem drobne, wiecznie odkładane naprawy, jak dopasowanie okna czy wymiana żarówek. Wyczyściłem i zaszyfrowałem swoje stare komputery, zmieniając je w niemą pozostałość po lepszych czasach. Starałem się wszystko uporządkować, żeby jak najbardziej ułatwić Lindsay życie albo uciszyć sumienie, które szarpało się między lojalnością wobec świata, który sobie na to nie zasłużył, a wobec zasługującej na to kobiety i rodziny, którą kochałem.

Wszystko było przeniknięte poczuciem końca, a jednak chwilami miałem wrażenie, że tego końca nie będzie, a mój plan się wali. Trudno mi było nakłonić dziennikarzy do umówienia się na spotkanie, głównie dlatego, że nie mogłem im powiedzieć, z kim się spotkają, a nawet, przynajmniej na razie, gdzie i kiedy ma to nastąpić. Musiałem liczyć się z ewentualnością, że nie przyjadą albo stawią się, ale potem się wycofają. Ostatecznie postanowiłem, że jeśli do tego dojdzie, po prostu zrezygnuję z planu; wrócę do pracy i Lindsay jakby nigdy nic i będę czekał na kolejną okazję.

Moje zwykle dwudziestominutowe dojazdy do pracy i powroty do domu zmieniły się w *wardriving** trwający nieraz nawet i dwie godziny, bo po znalezieniu sieci Wi-Fi przeszukiwałem różne kraje, starając się znaleźć odpowiednie miejsce na spotkanie z dziennikarzami. Miałem wrażenie, jakbym wybierał sobie więzienie, a raczej grób. Oczywiście żadne państwo Sojuszu Pięciorga Oczu nie wchodziło w grę. Nie mogłem też brać pod uwagę Europy, bo trudno było liczyć, że tamtejsze rządy postąpią zgodnie z międzynarodowym prawem dotyczącym ekstradycji osób oskarżonych o przestępstwa polityczne, gdy USA zacznie wywierać silny nacisk. Afryka i Ameryka Łacińska też się nie nadawały – wiedziałem, że Stany Zjednoczone nie raz bezkarnie przeprowadzały tam działania. Wykluczyłem Rosję, bo to była Rosja, i Chiny, bo to były Chiny. Oba te kraje znajdowały

się w strefie zakazanej. Gdybym tam pojechał, rząd USA nie musiałby nic więcej robić, żeby mnie zdyskredytować, niż wskazać palcem na mapę. Jeszcze gorzej by to wyglądało, gdybym pojechał na Bliski Wschód. Chwilami miałem wrażenie, że najtrudniejszym przedsięwzięciem mojego życia nie będzie splądrowanie zasobów NSA, tylko znalezienie miejsca spotkania na tyle niezależnego, żeby nie dopadł mnie tam Biały Dom, i na tyle swobodnego, by mi nie przeszkodzono.

Drogą eliminacji doszedłem do Hongkongu, który w sensie geopolitycznym miał status najbliższy ziemi niczyjej, a jednocześnie posiadał dynamiczne media i kulturę protestu, nie wspominając już o znacznie niefiltrowanym internecie. Hongkong był osobliwością, stosunkowo liberalną światową metropolią, której formalna autonomia uchroniłaby mnie i dziennikarzy przed publiczną reakcją Chin – przynajmniej tymczasowo – a jednocześnie przynależność do tego państwa znacznie zmniejszyłaby prawdopodobieństwo jednostronnej interwencji USA. Nie miałem żadnych gwarancji bezpieczeństwa, więc musiałem zadowolić się zapewnieniem, że starczy mi czasu. Przewidywałem, że wszystko to i tak może się źle skończyć, i miałem tylko nadzieję, że zdążę ujawnić zgromadzone materiały, zanim mnie złapią.

Tego dnia, gdy po raz ostatni obudziłem się obok Lindsay, wyjeżdżała na krótki wypad – kemping z przyjaciółmi, do czego sam ją zachęcałem. Leżeliśmy w łóżku i przytuliłem ją zbyt mocno, a ona z sennym zdumieniem spytała, dlaczego nagle stałem się taki uczuciowy. Przeprosiłem ją, mówiąc, że stale jestem tak bardzo zajęty, i dodałem, że będę za nią tęsknił i że jest najlepszą osobą, jaką w życiu spotkałem. Uśmiechnęła się, cmoknęła mnie w policzek i wstała, żeby się spakować.

Kiedy tylko wyszła za drzwi, zacząłem płakać, po raz pierwszy od wielu lat. Czułem się winny wszystkiego, oprócz tego, o co miał mnie

oskarżyć mój rząd. Szczególne poczucie winy miałem z powodu tych łez, bo wiedziałem, że moje cierpienie jest niczym w porównaniu z bólem, jaki sprawię ukochanej kobiecie, oraz cierpieniem i zażenowaniem, o jakie przyprawię rodzinę.

Ja przynajmniej wiedziałem, co się zdarzy. Lindsay natomiast wróci z kempingu i przekona się, że wyjechałem pod pretekstem podróży służbowej. Krótko potem przyjedzie moja matka, którą zaprosiłem, żeby nas odwiedziła, a było to dla mnie tak nietypowe, że z pewnością nastawiała się na zupełnie inną niespodziankę – może zaręczyliśmy się z Lindsay? Czułem się okropnie, że tak ją zwiodłem, i aż trudno mi było myśleć o jej wielkim rozczarowaniu, ale powtarzałem sobie, że było to usprawiedliwione. Mama zaopiekuje się Lindsay, a Lindsay mamą. Każdej potrzebna będzie siła tej drugiej, żeby razem przetrwały nadciągającą burzę.

Nazajutrz po wyjeździe Lindsay wziąłem dzień wolnego z powodu nagłej choroby, uzasadniając zwolnienie padaczką, po czym spakowałem niewielki bagaż i cztery laptopy: do poufnej komunikacji, do normalnej komunikacji, wabik i jeden nigdy niepodłączany do internetu. Smartfon zostawiłem na blacie kuchennym razem z notatnikiem, w którym napisałem długopisem: „Musiałem wyjechać służbowo. Kocham Cię”. I podpisałem się pseudonimem „Echo”, od mojego znaku wywoławczego. Potem pojechałem na lotnisko, gdzie za gotówkę kupiłem bilet na najbliższy lot do Tokio. W Tokio nabyłem kolejny bilet za gotówkę i 20 maja przybyłem do Hongkongu, miasta, gdzie po raz pierwszy poznał mnie świat.

---

* *Wardriving* to poruszanie się odpowiednio wyposażonym pojazdem w celu wyszukiwania i oznaczania działających sieci Wi-Fi (przyp. red.).

26_Hongkong|

Głęboki psychologiczny urok gier, które są po prostu seriami coraz trudniejszych wyzwań, wynika z przekonania, że można je wygrać. Najdobitniejszym tego przykładem jest dla mnie kostka Rubika, która zaspokaja powszechnie hołubioną fantazję: że jeśli włożysz odpowiednio dużo wysiłku i przećwiczysz każdą możliwą pozycję, wszystko, co wydaje się pomieszane i niezrozumiałe, nareszcie wskoczy na swoje miejsce i ułoży się w idealnym porządku; że ludzka pomysłowość wystarczy, by przeistoczyć nawet najbardziej dysfunkcyjny i chaotyczny system w logiczny, uporządkowany układ, w którym każda ze ścian trójwymiarowej bryły lśni idealnie jednorodną barwą.

Miałem plan – właściwie szereg planów – a ich cechą wspólną było przeświadczenie, że jeśli popełnię choć jeden błąd, zostanę pojmany.

Tak się jednak nie stało: wydostałem się z NSA, wydostałem się z kraju. Wygrałem. Wszystkie najtrudniejsze sytuacje, które potrafiłem sobie wyobrazić, miałem za sobą. Okazało się jednak, że są rzeczy, które przerastają moją wyobraźnię, na przykład to, że dziennikarze poproszeni o przybycie nie pojawią się. Cały czas przesuwali spotkanie, tłumaczyli się, przepraszali.

Wiedziałem, że Laura Poitras – jej wysłałem już kilka dokumentów i obiecałem o wiele więcej – była gotowa rzucić wszystko i lecieć z Nowego Jorku w dowolne miejsce na świecie, ale nie zamierzała podróżować do Hongkongu sama. Starała się namówić Glenna Greenwalda, żeby się zaangażował, żeby kupił nowy laptop i nie łączył go z internetem.

Żeby zainstalował programy szyfrujące, które ułatwiłyby nam komunikację. Mnie tymczasem pozostawało czekać w Hongkongu i spoglądać na wskazówki zegara odmierzające godziny, oraz na kalendarz i mijające kolejne dni, prosząc usilnie i błagając: „Przyjedźcie, zanim NSA zauważy, że zbyt długo nie wracam do pracy”. Trudno mi było pogodzić się z myślą, że mimo wszystkich starań mogłem utknąć w Hongkongu, nie osiągnąwszy niczego. Starałem się znaleźć w głębi serca cień sympatii dla dziennikarzy, którzy najwyraźniej byli zbyt zajęci albo zbyt wystraszeni, by wyznaczyć konkretną datę przyjazdu, ale potem przypominałem sobie, jak niewielka część materiałów, dla których ryzykowałem wszystko, trafiłaby do wiadomości publicznej, gdyby prasa dała się prześcignąć policji. Rozmyślałem o mojej rodzinie i Lindsay, oraz o tym, jaką głupotę popełniłem, oddając swoje życie w ręce osób, które nawet nie znały mojego nazwiska.

Zabarykadowałem się w pokoju w hotelu Mira; wybrałem ten obiekt ze względu na lokalizację pośrodku ruchliwej dzielnicy sklepowej i biznesowej. Wywiesiłem na drzwiach plakietkę „Nie przeszkadzać”, żeby odpędzić obsługę hotelową. Przez dziesięć dni nie opuszczałem pokoju, bo bałem się, że dam w ten sposób okazję zagranicznemu szpiegowi, by zakradł się do środka i założył podsłuch. Stawka była tak wysoka, że pozostało mi czekać. Zmieniłem swój azyl w skromnie wyposażone centrum operacyjne, niewidoczne serce sieci zaszyfrowanych tuneli internetowych, przez które słałem coraz bardziej histeryczne błagania do nieobecnych emisariuszy wolnej prasy. Później stawałem pod oknem i wyczekiwałem odpowiedzi, przyglądając się pięknemu parkowi, którego nie było mi dane odwiedzić. Do czasu, gdy Laura i Glenn nareszcie przybyli, zdążyłem spróbować wszystkich pozycji z hotelowego menu.

Nie chcę przez to powiedzieć, że przez ten tydzień nie robiłem nic poza wysyłaniem płaczliwych wiadomości. Starałem się też przygotować ostatni briefing mojego życia – przeczesywałem archiwum, rozważając, jak najlepiej przedstawić jego zawartość dziennikarzom w ograniczonym czasie, który wspólnie spędzimy. Było to interesujące zagadnienie: rozmawiać z osobami nieobeznanymi z technologią i niemal na pewno nastawionymi wobec mnie bardzo sceptycznie, by przekonać je, że rząd Stanów Zjednoczonych naprawdę inwigiluje cały świat, i wytłumaczyć im metody, którymi się posługuje. Zredagowałem słowniki z terminami związanymi ze sztuką internetowego szpiegostwa, takimi jak „metadane” i „nośnik informacji”, oraz glosariusze zawierające akronimy i skróty: CCE, SCC, DNI, NOFORN. Podjąłem decyzję, że spróbuję wykorzystać język dziennikarzy – nie będę się skupiał na technologiach i systemach, lecz na działaniu programów inwigilacyjnych – po prostu będę opowiadał historie. Nie potrafiłem jednak wybrać, które z tych historii opowiedzieć najpierw. Starałem się ułożyć najgorsze przestępstwa w stosownej kolejności, co chwila zmieniając zdanie.

Musiałem znaleźć sposób, by pomóc przynajmniej Laurze i Glennowi zrozumieć na przestrzeni kilku dni coś, czego pojęcie zajęło mi lata. Na tym jednak nie koniec: musiałem również sprawić, by zrozumieli, kim jestem i dlaczego zdecydowałem się na ten krok.

Drugiego czerwca Glenn i Laura nareszcie pojawili się w Hongkongu. Sądzę, że kiedy spotkali mnie w Mirze, początkowo byli zawiedzeni. W gruncie rzeczy nie muszę się tego domyślać, bo Glenn powiedział mi to wprost: oczekiwał kogoś starszego, jakiegoś udręczonego winą, nieuleczalnie chorego na raka, palącego na zakładkę alkoholika w odmętach depresji. Nie potrafił zrozumieć, jak to możliwe, że osoba tak młoda jak ja – kilkukrotnie pytał mnie o wiek – nie tylko miała dostęp do

tak poufnych dokumentów, ale była w takim stopniu gotowa poświęcić swoje życie. Ja za to nie pojmowałem, dlaczego spodziewali się siwego weterana, skoro udzieliłem im następujących instrukcji: pójdźcie do spokojnego zaułka przy restauracji hotelowej, tam, gdzie stoi kanapa obita imitacją skóry aligatora, i poczekajcie na faceta trzymającego kostkę Rubika. Co śmieszne, początkowo niepokoiłem się, czy dobrze robię, sięgając po tę technikę, ale kostka była jedynym stosunkowo niepowtarzalnym i łatwo rozpoznawalnym z odległości przedmiotem, który zabrałem ze sobą. Pomogła mi też ukryć stres wywołany koniecznością czekania na coś, co mogło okazać się niespodziewanym aresztowaniem.

Mój stres wyraźnie osiągnął szczyt niecałe dziesięć minut później, kiedy zaprowadziłem Laurę i Glenna do mojego pokoju numer 1014 na dziesiątym piętrze hotelu. Glenn ledwie zdążył zgodnie z moim poleceniem odłożyć swojego smartfona do lodówki w minibarze, zanim Laura zaczęła przestawiać źródła światła. Po chwili wypakowała swoją cyfrową kamerę. W szyfrowanych e-mailach, poprzez które się porozumiewaliśmy, zgodziłem się na filmowanie spotkania, ale nie byłem gotów na zderzenie z rzeczywistością.

Nic na świecie nie mogło przygotować mnie na moment, kiedy Laura skierowała na mnie obiektyw kamery. Leżałem na niepościelonym łóżku w ciasnym, zabałaganionym pokoju, którego nie opuszczałem przez dziesięć dni. Sądzę, że każdy ma za sobą podobne doświadczenie: im bardziej jesteś świadom tego, że ktoś cię nagrywa, tym mocniej dostrzegasz swoje wady. Samo wrażenie, że w twoim otoczeniu jest albo może być ktoś, kto skieruje na ciebie swój smartfon i dotknie przycisku nagrywania, wywołuje skrępowanie, nawet jeśli osoba ta jest dobrym znajomym. Mimo że obecnie prawie wszystkie moje kontakty z drugim człowiekiem odbywają się za pośrednictwem obiektywu i ekranu, wciąż nie jestem

pewien, które doświadczenie wywołuje we mnie silniejsze poczucie wyalienowania: oglądanie nagrań ze swoim udziałem czy bycie filmowanym. Staram się nie robić tego pierwszego, wszystkim nam jednak trudno dziś uniknąć tej drugiej okoliczności.

Ponieważ sytuacja już wcześniej była bardzo nerwowa, zesztywniałem. Czerwona dioda kamery Laury niczym laser snajpera przypominała mi, że w każdej chwili ktoś mógł wyważyć drzwi i mnie uprowadzić. A gdy tylko ta myśl opuściła moją głowę, zastąpiły ją rozmyślania o tym, jakie wrażenie zrobi to nagranie, kiedy będzie odtwarzane w sądzie. Zdałem sobie sprawę, że mogłem lepiej zadbać o pewne sprawy, na przykład porządniej się ubrać i ogolić. W pokoju nagromadziło się pełno brudnych talerzy i śmieci. Tu i ówdzie leżały pojemniki po chińszczyźnie i niedojedzone burgery, a po podłodze walały się brudne ubrania i wilgotne ręczniki.

W dynamice tej sytuacji było coś surrealistycznego. Stanąłem przed kamerą chwilę po tym, jak pierwszy raz w życiu poznałem reporterkę kręcącą filmy, i zostałem źródłem pierwszych dziennikarzy, jakich kiedykolwiek spotkałem. W dodatku kiedy po raz pierwszy opowiedziałem na głos o systemie masowej inwigilacji wykorzystywanym przez rząd Stanów Zjednoczonych, mówiłem do wszystkich osób na świecie, które miały dostęp do łącza internetowego. W ostatecznym rozrachunku mój niechlujny wygląd i nienaturalny sposób wypowiadania się nie miały znaczenia, za to nagranie Laury okazało się niezastąpione, bo pokazało światu to, co zdarzyło się w moim pokoju hotelowym tak, jak nie można było oddać tego w druku. Nagrań Laury z dni spędzonych wspólnie w Hongkongu nie da się zafałszować. Ich istnienie jest dowodem zarówno jej profesjonalizmu jako dokumentalistki, jak i dalekowzroczności.

Przez tydzień pomiędzy 3 a 9 czerwca tkwiłem odizolowany w moim pokoju w towarzystwie Glenna i jego kolegi z „Guardiana”, Ewena

MacAskilla, który dołączył do nas nieco później, ale pierwszego dnia. Rozmawialiśmy prawie bez przerwy, omawiając programy NSA, podczas gdy Laura krążyła wokół nas i filmowała. W odróżnieniu od dni, które mijały w nerwowym pośpiechu, nocami czułem się samotny i niepocieszony. Glenn i Ewen wracali do pobliskiego hotelu W i przekuwali swoje odkrycia w artykuły. Laura w tym czasie znikała montować nagrania i przygotowywać reportaże we współpracy z Bartem Gellmanem z „Washington Postu", któremu nie udało się dotrzeć do Hongkongu, ale pracował zdalnie na dokumentach otrzymanych od koleżanki.

Ja w tym czasie spałem albo próbowałem spać, a kiedy nie było takiej możliwości, włączałem jakiś anglojęzyczny kanał telewizyjny, na przykład BBC albo CNN, i oglądałem międzynarodową reakcję na wycieki. Piątego czerwca w „Guardianie" ukazał się pierwszy artykuł Glenna – na temat wyroku sądu FISA, który zezwolił NSA na pobór metadanych ze wszystkich rozmów telefonicznych obsługiwanych przez amerykańskiego operatora telekomunikacyjnego Verizon. Szóstego czerwca „Guardian" wypuścił artykuł Glenna o PRISM-ie; praktycznie równolegle ukazał się podobny reportaż Laury i Berta w „Washington Post". Wiedziałem – sądzę, że wszyscy wiedzieliśmy – że im więcej tekstów się ukaże, tym bardziej prawdopodobne będzie, że zostanę rozpoznany, szczególnie że zacząłem otrzymywać z biura prośby, bym przysłał informację o swoim stanie. Nie odpowiadałem. Glenn, Ewen i Laura bardzo współczuli mi tego, że siedzę na bombie zegarowej, ale ani na chwilę nie pozwolili sobie na to, by litość przyćmiła w nich potrzebę służenia prawdzie. Postanowiłem zatem iść za ich przykładem.

Wysiłki dziennikarzy, podobnie jak twórców filmów dokumentalnych, nie są w stanie oddać wszystkiego. Można dojść do ciekawych wniosków,

rozważając, co takie czy inne medium musi pominąć ze względu na konwencje i ograniczenia techniczne. Narracja Glenna, szczególnie ta w „Guardianie”, miała postać precyzyjnej jak laser prezentacji faktów odartej z zawziętości i pasji, które definiują jego osobowość. Styl Ewena lepiej odzwierciedlał jego charakter: był szczery, wdzięczny, cierpliwy i sprawiedliwy. Laurę, która wszystko widziała, ale rzadko dawała się zobaczyć, wyróżniały natomiast rezerwa płynąca z wszechwiedzy i sardoniczne poczucie humoru. Była w tym samym stopniu szpiegiem, co genialną artystką.

Podczas gdy wszystkie kanały telewizyjne i strony internetowe nadawały od rana do wieczora o ujawnionych tajemnicach, stało się jasne, że rząd Stanów Zjednoczonych zaprzągł całą swoją maszynerię do rozpoznania źródła dziennikarzy. Uważałem również za oczywiste, że kiedy mu się uda, wykorzysta twarz, którą znajdzie – moją – by uniknąć odpowiedzialności: zamiast odnieść się do sedna sprawy, będzie próbował podważyć wiarygodność i oczernić motywy sprawcy wycieku. Zważywszy na stawkę w grze, musiałem przejąć inicjatywę, nim będzie za późno. Wiedziałem, że jeśli nie wyjaśnię swoich postępowania i intencji, rząd zrobi to za mnie tak, że odwróci uwagę od własnych występków.

Jedyną szansę na zachowanie twarzy dawało mi ujawnienie tożsamości wcześniej. Zamierzałem przekazać mediom tylko tyle informacji na temat mojej osoby, ile wystarczyło, by zaspokoić ich rosnącą ciekawość, i jednoznacznie zadeklarować, że to nie ja jestem ważny, lecz pogwałcenie zasad amerykańskiej demokracji. Potem miałem zniknąć równie szybko, jak się pojawiłem. Taki w każdym razie ustaliliśmy plan.

Postanowiliśmy z Ewenem, że napisze artykuł o mojej karierze wywiadowczej, a Laura zasugerowała, żeby dołączyć moje oświadczenie w postaci wideo, które chciała nakręcić. Miałem wziąć na siebie osobistą

i pełną odpowiedzialność za podanie informacji, które ukazały się w reportażach na temat globalnej masowej inwigilacji.

Niestety, choć Laura kręciła nas przez cały tydzień (duża część efektów tej pracy trafiła do jej pełnometrażowego filmu dokumentalnego *Citizenfour*), nie miała czasu, żeby wyszukać w zgromadzonym materiale fragmentów, gdzie wypowiadam się z sensem, spoglądając w stronę kamery. Zaproponowała zatem, byśmy nakręcili od nowa moje pierwsze oświadczenie, które zaczęła filmować, kiedy tylko skończyła mówić – to zaczynające się od słów: „Yyy, nazywam się Ed Snowden. Mam, yyy, dwadzieścia dziewięć lat".

Witaj, świecie.

Ani razu nie zdarzyło mi się żałować, że odsłoniłem kulisy i ujawniłem swoją tożsamość, ale gdybym miał to zrobić jeszcze raz, zadbałbym o poprawniejszą dykcję i o to, by mieć w głowie lepszy plan na przyszłość. W rzeczywistości bowiem nie miałem żadnego. Prawie w ogóle nie zastanawiałem się, co zrobić po ujawnieniu materiałów – głównie dlatego, że powodzenie tego przedsięwzięcia wydawało mi się tak mało prawdopodobne. Zależało mi tylko na tym, żeby przekazać fakty do ogólnej wiadomości: zakładałem, że upowszechniając je, skażę się na łaskę opinii publicznej. Jedyną strategią był brak strategii, ponieważ zaplanowanie dalszych kroków w dowolnej postaci mogło podważyć wiarygodność ujawnionych informacji.

Gdybym zorganizował sobie podróż lotniczą do konkretnego kraju, żeby ubiegać się w nim o azyl, rząd nazwałby mnie szpiegiem na rzecz tego państwa. Z kolei gdybym wrócił do Stanów, mógłbym liczyć wyłącznie na aresztowanie na lotnisku i oskarżenie za naruszenia prawa opisane w Espionage Act. Zyskałbym jedynie możliwość udziału w pokazowym

procesie, w którym nie miałbym szans na rzeczową obronę – odbyłaby się farsa z zakazem dyskusji o najważniejszych faktach.

Poważne przeszkody na drodze do sprawiedliwości są zasadniczą słabością naszego prawa – słabością stworzoną umyślnie przez rząd. Osobie w mojej sytuacji nie wolno nawet uzasadniać przed sądem, że wyjawienie informacji dziennikarzom było społecznie korzystne. Nawet dziś, lata po zdarzeniu, nie zezwolono by mi posłużyć się argumentem, że reportaże opublikowane na podstawie uzyskanych ode mnie informacji zmusiły Kongres do zmiany pewnych praw regulujących działalność wywiadowczą, przekonały sądy do uznania określonego programu powszechnej inwigilacji za nielegalny i nakłoniły prokuratora generalnego oraz prezydenta Stanów Zjednoczonych do przyznania, że masowa inwigilacja zdecydowanie powinna stać się tematem publicznej debaty, która w ostatecznym rozrachunku wzmocni nasz kraj. Wszystkie te fakty zostałyby uznane nie tylko za pozbawione znaczenia, lecz także niedopuszczalne w procesie, w którym musiałbym wziąć udział, gdybym wrócił do domu. Rząd musiałby udowodnić przed sądem tylko to, że ujawniłem dziennikarzom tajne informacje, co nie podlegało dyskusji. Dlatego wszyscy twierdzący, że powinienem wrócić do Stanów i oddać się w ręce sprawiedliwości, są zasadniczo zdania, że powinienem powrócić, żeby otrzymać wyrok, który – dziś tak samo jak wtedy – z pewnością byłby okrutny. Kara za ujawnienie informacji objętych klauzulą „ściśle tajne”, nieważne, czy za przekazanie ich wrogim szpiegom, czy amerykańskim dziennikarzom, wynosi do dziesięciu lat za każdy dokument.

Odkąd nagranie Laury z moją osobą w roli głównej ukazało się na stronie „Guardiana” – 9 czerwca – stałem się celem. Miałem świadomość, że instytucje, które ośmieszyłem, nie spoczną, dopóki moja głowa nie znajdzie się w czarnym worku, a ręce i nogi w kajdankach. I że do tego

czasu – a możliwe, że nawet dłużej – będą nękać moich najbliższych i szargać moją reputację, szczegółowo rozgrzebywać moje życie i karierę w poszukiwaniu informacji (albo okazji do dezinformacji), żeby móc mnie oczernić.

Wiedziałem mniej więcej, jak ten proces przebiega, ponieważ czytałem utajnione raporty wywiadowcze z podobnych postępowań i przestudiowałem przypadki innych sygnalistów i sprawców wycieków. Znałem losy bohaterów pokroju Daniela Ellsberga i Anthony'ego Russo oraz bliższych współczesności przeciwników rządowej tajności, takich jak Thomas Tamm, prawnik związany z Biurem Polityki i Kontroli nad Wywiadem Departamentu Sprawiedliwości; posłużył on za źródło większości reportaży na temat podsłuchów bez nakazu sądowego, które ukazały się w połowie pierwszej dekady XXI wieku. Pamiętałem też o Drake'u, Binneyu, Wiebem i Loomisie – godnym ery cyfrowej następcom Perry'ego Fellwocka, który w 1971 roku wyjawił prasie istnienie NSA; rząd utrzymywał to wcześniej w tajemnicy, czym sprawił, że senacka komisja Churcha (prekursorka obecnej Komisji do spraw Wywiadu Senatu Stanów Zjednoczonych) podjęła próbę ograniczenia mandatu agencji do inwigilacji tylko zagranicznych sygnałów elektromagnetycznych. Oczywiście muszę wspomnieć o szeregowej US Army Chelsea Manning, która za przestępstwo wyjawienia amerykańskich zbrodni wojennych została postawiona przed trybunałem wojskowym i skazana na trzydzieści pięć lat więzienia. Spędziła za kratami siedem lat, a jej wyrok złagodzono dopiero po międzynarodowym skandalu wywołanym tym, jak traktowano ją podczas przetrzymywania w izolatce.

Wszystkich tych ludzi, bez względu na to, czy groziło im więzienie, spotkała gwałtowna reakcja, w większości wypadków surowa i będąca skutkiem tego samego zjawiska, które dopiero co pomogli zdemaskować:

nadużyć w dziedzinie inwigilacji. Jeśli kiedykolwiek wyrazili złość w prywatnej komunikacji, przypinano im etykietkę malkontenta. Jeżeli kiedyś odwiedzili psychiatrę albo psychologa czy też po prostu wypożyczyli z biblioteki książkę ze zbliżonej dziedziny, nazywano ich niestabilnymi umysłowo. Jeśli choć raz się upili, robiono z nich alkoholików. Jeżeli zdarzyło im się zdradzić żonę, musieli zostać od razu seksualnymi dewiantami. Niejeden z nich stracił dom i wszystkie oszczędności. Instytucji łatwiej jest zszargać czyjąś reputację niż konstruktywnie odnieść się do uzasadnionej etycznie opozycji – aby rozwiązać problem, służby wywiadowcze muszą jedynie zajrzeć do kartoteki danej osoby i wyolbrzymić posiadane dowody albo, jeśli takowe nie istnieją, sfabrykować je.

Byłem przekonany, że mój rząd zapała świętym oburzeniem, i równie mocno wierzyłem, że mogę liczyć na wsparcie rodziny i Lindsay. Miałem pewność, że Lindsay zrozumie – niekoniecznie wybaczy, ale zrozumie – moje zachowanie w ostatnim okresie. Pocieszałem się myślami o miłości najbliższych: pomogły mi pogodzić się z faktem, że nie pozostało mi nic więcej do zrobienia, że nie miałem więcej planów. Mogłem co najwyżej, może trochę idealistycznie, uwierzyć, że również moi współobywatele, kiedy w pełni uświadomią sobie zakres masowej inwigilacji prowadzonej przez amerykański rząd, poczują, że mają prawo żądać sprawiedliwości, zmobilizują się i w ten sposób zadecydują o moim losie. Był to poniekąd akt najwyższej wiary: skoro nie mogłem ufać praktycznie nikomu, musiałem zaufać wszystkim.

Kilka godzin po ukazaniu się nagrania w „Guardianie” jeden ze stałych czytelników Glenna z Hongkongu zwrócił się do niego i zaproponował, że skontaktuje mnie z Robertem Tibbo i Jonathanem Manem, dwoma

miejscowymi adwokatami, którzy niedługo później zgodzili się zająć moją sprawą. To oni pomogli mi wydostać się z hotelu Mira, kiedy prasa – namierzywszy mnie wreszcie – rozpoczęła oblężenie głównego wejścia. Glenn wziął na siebie rolę dywersanta i wyszedł frontowymi drzwiami, gdzie natychmiast obległy go setki kamer i mikrofonów, a ja zostałem w tym czasie bezceremonialnie wypchnięty przez jedno z wielu pozostałych wyjść, za którymi znajdowała się kładka prowadząca do centrum handlowego.

Polubiłem Roberta. Być jego klientem znaczy zostać jego przyjacielem na całe życie – jest idealistą i niezmordowanym wojownikiem o prawa osób spisanych na straty. Jeszcze bardziej niż umiejętnościami prawniczymi zaimponował mi jednak kreatywnością, którą wykazał się w szukaniu dla mnie kryjówki. Podczas gdy dziennikarze przeczesywali wszystkie pięciogwiazdkowe hotele, Robert zabrał mnie do jednej z najbiedniejszych dzielnic miasta i przedstawił kilku pozostałym klientom – członkom dwunastotysięcznej zapomnianej społeczności uchodźców zamieszkującej Hongkong, zresztą pod presją Chin region ten hańbi się, przyznając prawo stałego pobytu ledwie jednemu procentowi ubiegających się o nie. W normalnych warunkach nie wymieniłbym z nazwiska osób, które mi pomogły, ale tym razem zrobię to, ponieważ same odważnie wyjawiły swoją tożsamość prasie. Byli to: Vanessa Mae Bondalian Rodel z Filipin oraz Ajith Pushpakumara, Supun Thilina Kellapatha i Nadeeka Dilrukshi Nonis ze Sri Lanki.

Ta czwórka nieskończenie serdecznych i szczodrych ludzi potraktowała mnie z niebywałą wspaniałomyślnością. Solidarność, którą mi okazali, nie miała wymiaru politycznego, lecz ludzki, i do końca życia będę miał wobec nich dług wdzięczności. Nie przejęli się tym, kim jestem, ani jakie niebezpieczeństwo może im grozić za udzielenie mi pomocy – interesowało

ich tylko to, że oto mają przed sobą człowieka w potrzebie. Wiedzieli z własnego doświadczenia, jakie to uczucie zostać zmuszonym do szalonej ucieczki przed śmiertelnym zagrożeniem, bo mieli za sobą wojskowe tortury, gwałt, przemoc – przeżycia o wiele gorsze od tego, co spotkało lub mogło spotkać mnie. Wpuścili do swoich domów wyczerpanego obcego mężczyznę, a kiedy zobaczyli moją twarz w telewizji, nie wycofali się. Zamiast tego obdarzyli mnie uśmiechem i zapewnili, że nie wypuszczą mnie spod swoich skrzydeł.

Choć dysponowali ograniczonymi środkami – Supun, Nadeeka, Vanessa i dwie dziewczynki mieszkali w rozsypującym się, ciasnym mieszkanku mniejszym niż mój pokój w Mirze – dzielili się ze mną wszystkim i bez ograniczeń, odrzucając moje oferty zapłaty za gościnę z taką zawziętością, że musiałem chować pieniądze w pokoju, by je przyjęli. Karmili mnie, pozwolili mi się kąpać, dali mi miejsce do spania i chronili mnie. Do końca życia nie będę umiał opisać słowami, ile to dla mnie znaczyło, że ci, którzy mieli tak mało, dali mi tak wiele i zaakceptowali mnie bez oceniania, choć spędziłem większość czasu przyczajony w kącie niczym uliczny kot, ślizgając się po Wi-Fi odległych hoteli za pomocą specjalnej anteny o wyglądzie fascynującym dzieci.

Ich gościnność i przyjaźń były wielkim darem, podobnie jak dla świata darem jest samo istnienie takich ludzi. Dlatego jest mi niezmiernie przykro, że choć minęło wiele lat, sprawy Ajitha, Supun, Nadeeki i córki Nadeeki wciąż się ciągną. Mojemu uwielbieniu dla nich wszystkich dorównuje wyłącznie mój żal wobec biurokratów z Hongkongu, którzy wciąż odmawiają im podstawowej godności w postaci azylu. Jeśli aparat państwowy nie uważa osób tak fundamentalnie porządnych i bezinteresownych za godne ochrony, to płynie z tego wniosek, że sam jest niegodny szacunku. Nadzieję daje mi tylko informacja, którą otrzymałem

dosłownie chwilę przed oddaniem niniejszej książki do druku, że Vanessie i jej córce przyznano azyl w Kanadzie. Z niecierpliwością wyczekuję dnia, kiedy będę mógł odwiedzić wszystkich moich przyjaciół z Hongkongu w ich nowych domach, gdziekolwiek się znajdą, i zastąpić stare wspomnienia przyjemniejszymi – wspomnieniami wolnych ludzi.

Czternastego czerwca rząd Stanów Zjednoczonych wniósł wobec mnie niejawne oskarżenie na mocy Espionage Act, a 21 czerwca formalnie zażądał mojej ekstradycji. Zdałem sobie sprawę, że najwyższy czas wyjechać. Tak się złożyło, że były to moje trzydzieste urodziny.

Mniej więcej wtedy, kiedy Departament Stanu USA wysłał żądanie ekstradycji, moi prawnicy otrzymali odpowiedź na prośbę o wsparcie ze strony Wysokiego Komisarza Narodów Zjednoczonych do spraw uchodźców. Brzmiała: nie da się nic dla mnie zrobić. Rząd Hongkongu, nie wiadomo, czy pod presją Chin, czy też nie, oparł się wszelkim próbom ONZ zapewnienia mi międzynarodowej ochrony na jego terytorium, a na dodatek oświadczył, że w pierwszej kolejności będzie zmuszony uznać roszczenia kraju, którego obywatelstwo posiadam. Innymi słowy miałem wrócić do domu i rozmawiać z przedstawicielami Narodów Zjednoczonych z więzienia.

Nie byłem już zdany na pastwę losu, tylko niemile widziany. Jeśli chciałem opuścić Hongkong jako wolny człowiek, musiałem zrobić to natychmiast.

Dokładnie wyczyściłem swoje cztery laptopy i zniszczyłem klucz kryptograficzny, raz na zawsze odbierając sobie i osobom, które mogłyby zastosować wobec mnie przymus, dostęp do rządowych dokumentów. Następnie spakowałem nieliczne ubrania, jakie miałem ze sobą, i wyruszyłem w drogę. Nie byłem już bezpieczny w „pachnącym porcie”.

27_Moskwa|

Jak na nadmorskie państwo na północno-zachodnim krańcu Ameryki Południowej, oddalone o pół globu od Hongkongu, Ekwador znajduje się w samym centrum wszystkiego – nie bez powodu zresztą jego nazwa oznacza równik. Większość mieszkańców Ameryki Północnej słusznie powiedziałaby, że to mały kraj, a niektórzy wiedzieliby może, że był uciskany na przestrzeni dziejów. Ale myli się ten, kto sądzi, że to zaścianek. Prezydentem Ekwadoru w 2007 roku został Rafael Correa, wyniesiony na fali zwycięstw liderów socjalizmu demokratycznego w Boliwii, Argentynie, Brazylii, Paragwaju i Wenezueli, wzbierającej od końca XX i na początku XXI wieku. Po objęciu władzy Correa przedstawił liczne inicjatywy mające na celu przeciwstawienie się imperialistycznym zakusom USA w tym regionie i zlikwidowanie skutków ich działań. Takim posunięciem, odzwierciedlającym przy okazji jego ekonomiczne wykształcenie i doświadczenie zdobyte przez polityka na stanowisku ministra finansów, było ogłoszenie, że Ekwador uznaje swój dług narodowy za bezprawny – w prawie międzynarodowym określana się go *odious debt* (długiem niemoralnym). Chodzi o dług państwowy zaciągnięty na przykład przez reżim totalitarny lub w wyniku despotycznej imperialistycznej polityki handlowej. Uznaje się, że tego typu długu nie trzeba spłacać. Dzięki temu oświadczeniu Correa uwolnił obywateli od kilkudziesięciu lat problemów gospodarczych, ale jednocześnie przysporzył sobie wrogów wśród finansistów, którzy w dużej mierze wpływają na politykę zagraniczną USA.

W każdym razie w 2013 roku Ekwador czynnie popierał prawo azylu politycznego. Chyba najbardziej znanym przypadkiem zastosowania go w praktyce było udzielenie schronienia Julianowi Assange'owi z WikiLeaks w ambasadzie Ekwadoru w Londynie. Osobiście nie miałem ochoty mieszkać w ambasadzie, może dlatego, że już w jednej pracowałem. Niemniej moi prawnicy w Hongkongu doszli do wniosku, że w obecnych okolicznościach Ekwador wydaje się najlepszym wyborem, ponieważ ten kraj obroni moje prawo do azylu politycznego i nie da się zastraszyć hegemonowi rządzącemu tamtejszą półkulą. Mój rozrastający się przez cały czas tymczasowy zespół prawników, dziennikarzy, specjalistów od technologii i aktywistów zgodził się z tym poglądem. Miałem nadzieję, że uda mi się dotrzeć do samego Ekwadoru, a nie jego przedstawicielstwa.

Skoro mój rząd zdecydował się postawić mi zarzuty z tytułu ustawy o szpiegostwie, zostałem oskarżony o przestępstwo polityczne, czyli takie, gdzie ofiarą jest państwo, a nie osoba. Zgodnie z międzynarodowym prawem humanitarnym takie oskarżenia na ogół nie pociągają za sobą ekstradycji, bowiem często są autorytarnymi próbami stłumienia zgodnego z prawem sprzeciwu. Teoretycznie osoby sygnalizujące nieprawidłowości w działaniu państwowych instytucji powinny niemal wszędzie otrzymywać ochronę przed ekstradycją. W rzeczywistości jednak rzadko tak się dzieje, szczególnie gdy za skrzywdzone państwo uważa się USA. Stany Zjednoczone szczycą się wspieraniem demokracji na całym świecie, ale nie wspominają o tajnej flocie samolotów na prywatnych umowach, wykorzystywanej do bezprawnych ekstradycji określanych mianem wydania w trybie nadzwyczajnym, co dla wszystkich pozostałych oznacza po prostu porwanie.

Pomagający mi zespół skontaktował się z większością państw, od Islandii po Indie, chcąc ustalić, czy poszczególne państwa zastosują się do

zakazu ekstradycji osób oskarżonych o przestępstwa polityczne i zobowiążą do nieinterweniowania, gdybym podróżował przez ich teren. Wkrótce przekonaliśmy się, że nawet najbardziej demokratyczne podmioty boją się gniewu rządu USA. Prywatnie urzędnicy wyrażali solidarność, ale niechętnie wspominali – nawet nieoficjalnie – o jakichkolwiek gwarancjach. Wspólnym mianownikiem wszystkich porad, które otrzymywałem, była sugestia, żeby lądować tylko w krajach bez umowy o ekstradycję z USA oraz unikać lotów, których trasa przebiega przez przestrzeń powietrzną państw znanych ze współpracy wojskowej z tym krajem. Pewien rozmówca, chyba z Francji, stwierdził, że moje szanse na dotarcie do celu znacznie wzrosną, jeśli postaram się o *laissez-passer*, uznawany przez ONZ dokument upoważniający do podróży w jedną stronę, często wydawany uchodźcom, żeby umożliwić im przekroczenie granicy. Łatwiej powiedzieć niż zrobić.

Do naszego grona dołączyła też Sarah Harrison, dziennikarka i redaktorka WikiLeaks. Kiedy tylko podano w wiadomościach, że pewien Amerykanin zdemaskował globalny system masowej inwigilacji, natychmiast wsiadła do samolotu do Hongkongu. Dysponując bogatym doświadczeniem zdobytym w WikiLeaks, a szczególnie podczas zajmowania się problemami Assange’a, mogła udzielić mi najskuteczniejszych rad dotyczących azylu politycznego. Dodatkowym atutem były jej rodzinne powiązania ze społecznością prawniczą w Hongkongu.

Assange’owi przez dłuższy czas zarzucano, że pragnął udzielić mi wsparcia z egoistycznych pobudek, ale ja uważam, że szczerze zależało mu przede wszystkim na jednym – by pomóc mi uniknąć pojmania. Możliwość dania w ten sposób prztyczka w nos rządowi USA była dodatkową korzyścią, nie celem. Nie przeczę, że Assange bywa wyrachowany, próżny,

kapryśny, a nawet okrutny – po ostrej kłótni zaledwie w miesiąc po naszej pierwszej rozmowie, oczywiście pisemnej, nigdy więcej się z nim nie kontaktowałem – ale autentycznie uważa się za bojownika biorącego udział w historycznych zmaganiach o prawo ogółu do wiedzy, i zrobi wszystko, żeby te boje wygrać. Dlatego uważam, że nadmiernym uproszczeniem jest interpretowanie jego pomocy jako autopromocji czy machinacji. Moim zdaniem ważniejsze dla niego było ustanowienie kontrprzykładu dla sprawy najsłynniejszego źródła WikiLeaks, Chelsea Manning, skazanej na bezprecedensowy wyrok trzydziestu pięciu lat więzienia. Był to niezwykle odstraszający incydent dla innych demaskatorów. Nigdy nie byłem i nie będę źródłem Assange'a, ale moja sytuacja dawała mu okazję do naprawienia zła. Co prawda nie mógł w żaden sposób pomóc Chelsea Manning, ale był zdeterminowany, żeby za pośrednictwem Sarah zrobić wszystko dla ratowania mnie.

Początkowo ostrożnie podchodziłem do angażowania Sarah. Laura jednak przekonała mnie, że to poważna, kompetentna i co najważniejsze niezależna osoba – była jedną z niewielu w WikiLeaks, która miała odwagę otwarcie nie zgadzać się z Assange'em. Ostrożność swoją drogą, ale byłem w trudnej sytuacji, a jak kiedyś pisał Hemingway, jedynym sposobem, żeby inni stali się godni zaufania, jest im zaufać.

Laura poinformowała mnie o obecności Sarah w Hongkongu zaledwie na dzień przed tym, jak ta skontaktowała się ze mną szyfrowanym kanałem; dzień czy dwa dni później spotkałem się z Sarah osobiście. Trochę mylą mi się te daty, wybacz – po prostu wówczas jedna szaleńcza doba zlewała się z kolejną. Sarah od samego przylotu działała wyjątkowo aktywnie. Wprawdzie nie była prawniczką, ale miała bogate doświadczenie w kwestiach, które nazywam interpersonalnymi lub prawie oficjalnymi niuansami unikania ekstradycji. Sarah spotkała się z miejscowymi

prawnikami broniącymi praw człowieka w celu uzyskania ich niezależnych opinii, a ja byłem pod ogromnym wrażeniem jej tempa i przezorności. Dzięki kontaktom z WikiLeaks oraz ogromnej odwadze Fidela Narvaeza, wówczas konsula Ekwadoru w Londynie, zdobyła na moje nazwisko *laissez-passer* – dokument, który miał zapewnić mi dotarcie do Ekwadoru. Konsul wystawił go w trybie wyjątkowym, bo nie było czasu na oficjalne zatwierdzenie przez instytucje rządowe w kraju. Jak tylko *laissez-passer* znalazł się w naszych rękach, Sarah wynajęła samochód, żeby zawiózł nas na lotnisko.

I tak ją poznałem – w ruchu. Chciałbym powiedzieć, że rozpocząłem naszą znajomość od podziękowania jej, ale w rzeczywistości pierwsze, co mi się nasunęło, to: „Kiedy ostatnio spałaś?”. Wyglądała na tak samo wykończoną i zaniedbaną jak ja. Wgapiła się w okno, jakby starała się znaleźć odpowiedź, ale w końcu tylko pokręciła głową: „Nie mam pojęcia”.

Obydwoje byliśmy silnie przeziębieni, naszą uważną rozmowę co chwilę przerywały kichnięcia lub kaszel. Sarah sama przyznała, że do zaangażowania się w pomoc skłoniło ją w większym stopniu sumienie niż ideologiczne przesłanki jej pracodawcy. I rzeczywiście odniosłem wrażenie, że na jej postępowanie w mniejszym stopniu wpływał zawzięty opór Assange’a wobec władzy centralnej niż jej własne przekonanie, że ci, którzy nazywają się współczesnymi dziennikarzami, służą interesom rządów zamiast je kwestionować. Przez cały czas, gdy pędziliśmy na lotnisko, i później, podczas odprawy oraz kontroli paszportowej przed pierwszym z trzech zaplanowanych przelotów, czekałem, aż mnie o coś poprosi – o cokolwiek, choćby o wygłoszenie oświadczenia o Assange’u lub jego organizacji. Ale tego nie zrobiła. Wyraziła za to ochoczo opinię, że byłem głupcem, wierząc, że konglomeraty medialne uczciwie nadzorują śluzę pomiędzy społeczeństwem a wiedzą. Zawsze będę podziwiać

szczerość Sarah zarówno za to bezpośrednie stwierdzenie, jak i wiele innych.

Podróżowaliśmy do Quito w Ekwadorze przez Moskwę, Hawanę i Caracas z tej prostej przyczyny, że była to jedyna bezpieczna trasa. Nie istniały bezpośrednie loty z Hongkongu do Quito, a wszystkie inne połączenia pośrednie prowadziły przez przestrzeń powietrzną należącą do USA. Martwiła mnie długa przerwa w podróży w Moskwie, gdzie mieliśmy czekać niemal dwadzieścia godzin na lot do Hawany, ale znacznie bardziej bałem się następnego etapu. Lot z Rosji na Kubę przecinał przestrzeń powietrzną NATO. Nie byłem szczególnie zachwycony perspektywą przelotu nad Polską, która w trakcie całego mojego życia robiła wszystko, żeby zadowolić amerykański rząd. Gościła nawet tajne więzienia CIA, gdzie moi byli koledzy z wywiadu stosowali wobec więźniów „wzmocnione techniki przesłuchań”, co jest eufemizmem z czasów ery Busha oznaczającym tortury.

Ściągnąłem czapkę jak najniżej na czoło, żeby mnie nie rozpoznano, a Sarah była moimi oczami. Wzięła mnie pod rękę i doprowadziła do bramki, gdzie czekaliśmy aż do wejścia na pokład. To była ostatnia chwila, kiedy mogła się wycofać, i powiedziałem jej to.

– Nie musisz tego robić – odezwałem się.

– Czego?

– Chronić mnie, tak jak teraz.

Sarah zesztywniała.

– Wyjaśnijmy sobie jedno – powiedziała, gdy wsiadaliśmy. – Ja cię nie chronię. Nikt nie potrafi cię ochronić. Jestem tu po to, żeby utrudnić innym ingerencję. Żeby wszyscy zachowywali się przyzwoicie.

– Czyli jesteś moim świadkiem – podsumowałem.

Uśmiechnęła się cierpko.

– Ktoś musi być ostatnią osobą, która widziała cię żywego. Równie dobrze mogę to być ja.

Wprawdzie przeszliśmy już trzy punkty, gdzie najbardziej obawiałem się zatrzymania (odprawę, kontrolę paszportową i bramkę), ale na pokładzie też nie czułem się bezpiecznie. Nie chciałem pozwolić sobie na nieostrożność. Usiadłem na miejscu przy oknie, a Sarah obok mnie, żeby zasłonić mnie przed wzrokiem pasażerów z naszego rzędu. Miałem wrażenie, że minęła wieczność, zanim drzwi kabiny zamknięto, odjechał rękaw lotniczy i ruszyliśmy z miejsca. Ale zanim samolot wjechał z płyty lotniska na pas startowy, zatrzymaliśmy się z ostrym szarpnięciem. Zdenerwowałem się. Przyciskając daszek czapki do szyby, starałem się dostrzec, czy nie błyskają niebieskie światła, i nasłuchiwałem, czy nie wyją syreny. Wyglądało na to, że znowu przyszło mi czekać. To czekanie chyba nigdy się nie skończy. A jednak nagle samolot znów zaczął kołować i skręcił, a wtedy zorientowałem się, że po prostu byliśmy na końcu długiej kolejki do startu.

W miarę jak samolot się wznosił, wzbierała też we mnie otucha, ale trudno mi było uwierzyć, że udało mi się wydostać z Hongkongu. Kiedy znaleźliśmy się w powietrzu, rozluźniłem dłonie zaciśnięte z całej siły na udach i zapragnąłem wyciągnąć swoją szczęśliwą kostkę Rubika z bagażu. Ale wiedziałem, że nie mogę, bo to z pewnością zwróciłoby na mnie uwagę. Dlatego odchyliłem się do tyłu, znów naciągnąłem czapkę na oczy i przyglądałem się spikselizowanej trasie naszego lotu na ekranie umieszczonym w oparciu przede mną. Trasa wiodła przez Chiny, Mongolię i Rosję, a żadne z tych państw nie pali się do wyświadczania przysług amerykańskiemu Departamentowi Stanu. Trudno było jednak przewidzieć, co zrobi rząd Rosji, kiedy już wylądujemy. Pewne było tylko, że wezmą nas do kontroli, żeby móc przeszukać moje, teraz już wyczyszczone laptopy

i pustą torbę. Liczyłem, że przed bardziej nieprzyjemnym potraktowaniem ochroni nas fakt, że świat patrzył, a moi prawnicy i ci z WikiLeaks znali naszą trasę.

Dopiero kiedy znaleźliśmy się w przestrzeni powietrznej Chin, uświadomiłem sobie, że nie będę w stanie odpocząć, dopóki jasno nie zadam Sarah tego pytania:

– Dlaczego mi pomagasz?

Zniżyła głos, jakby starała się zdusić uczucia, i odparła, że chciała, bym więcej osiągnął. Nie wyjaśniła dokładniej, o co jej konkretnie chodzi, a ja mogłem tylko uznać tę odpowiedź za oznakę jej dyskrecji i szacunku.

Ale dodało mi to otuchy na tyle, że w końcu zasnąłem.

Dwudziestego trzeciego czerwca wylądowaliśmy na lotnisku Szeremietiewo, gdzie mieliśmy zatrzymać się na dwadzieścia godzin w oczekiwaniu na kolejny samolot. Postój ten trwa już sześć lat. Wygnanie to niekończąca się przerwa w podróży.

Pracownicy wywiadu, CIA w szczególności, są dobrze szkoleni, żeby unikać kłopotów podczas odprawy celnej i paszportowej. Dbają o to, jak być ubranym, jak się zachowywać, jakie przedmioty mieć w bagażu i w kieszeniach, i zwracają uwagę, co o nich mówią. Cel to stać się najnudniejszą osobą w kolejce i postarać się o twarz, która w ogóle nie zapada w pamięć. Żaden z tych zabiegów nie ma jednak znaczenia, kiedy nazwisko figurujące w twoim paszporcie przewija się przez wszystkie dzienniki telewizyjne.

Podałem moją małą niebieską książeczkę facetowi o niedźwiedziej posturze w okienku paszportowym, ten ją zeskanował i przewertował strony. Sarah dzielnie stała za moimi plecami. Ponieważ obserwowałem, ile czasu zajmuje odprawa oczekującym w kolejce przed nami, wiedziałem, że

przebywamy przy okienku za długo. Po chwili urzędnik podniósł telefon, wymamrotał kilka słów po rosyjsku i prawie natychmiast – o wiele za szybko – podeszło do nas dwóch ochroniarzy w garniturach. Musieli czekać. Oficer na przedzie wziął moją niebieską książeczkę od faceta w okienku i nachylił się ku mnie.

– Jest problem z paszportem – powiedział. – Proszę pójść z nami.

Sarah natychmiast stanęła obok mnie, a z jej ust dobył się potok szybko artykułowanego angielskiego:

– Jestem doradcą prawnym tego pana. Będę mu towarzyszyć na każdym kroku. Idę z wami. Zgodnie z…

Zanim zdążyła wyrecytować nazwy odpowiednich postanowień ONZ i kodycyli genewskich, oficer uniósł dłoń, zerkając na kolejkę. Powiedział:

– Dobra, jasne. Dobra. Proszę.

Nie wiem, czy w ogóle zrozumiał, co mówiła. Było oczywiste, że chce uniknąć sceny.

Ochroniarze poprowadzili nas żywym krokiem w kierunku pomieszczenia, które – zakładałem – miało służyć dokładniejszym przeszukaniom, a tymczasem okazało się jedną z ekskluzywnych poczekalni biznesowych mieszczących się na terenie Szeremietiewa. Była to specjalna sala klasy biznesowej albo pierwszej, praktycznie pusta, pomijając kilka osób, które nieświadome niczego relaksowały się na luksusowych fotelach. Sarah i mnie pokierowano obok nich i wzdłuż korytarza, do swego rodzaju salki konferencyjnej pełnej mężczyzn w szarych garniturach zebranych wokół stołu. Było ich sześciu, może siedmiu, i wszyscy mieli wojskowe fryzury. Jeden z nich siedział w pewnej odległości od pozostałych i trzymał długopis – domyśliłem się, że jego rola polega na robieniu notatek – był kimś w rodzaju sekretarza. Miał przed sobą teczkę z jakimiś papierami; na okładce widniało jednokolorowe godło

o znaczeniu doskonale dla mnie zrozumiałym mimo nieznajomości rosyjskiego: były to miecz i tarcza, symbole najważniejszej rosyjskiej agencji wywiadowczej – FSB (Federalnej Służby Bezpieczeństwa). Podobnie jak w przypadku FBI w Stanach Zjednoczonych, funkcją FSB jest nie tylko szpiegowanie i prowadzenie dochodzeń, lecz również dokonywanie aresztowań.

Pośrodku stołu siedział starszy mężczyzna w garniturze lepszego gatunku od pozostałych. Biel włosów na jego głowie jaśniała jak nimb władzy. Jednoznacznym zamaszystym gestem wskazał Sarah i mnie, byśmy usiedli naprzeciw niego, i uśmiechnął się w sposób, który dał mi do zrozumienia, że mam do czynienia z doświadczonym oficerem prowadzącym czy jakkolwiek nazywano w Rosji jego funkcję. Służby wywiadowcze całego świata są pełne takich postaci – oddanych sprawie aktorów, którzy próbują różnych emocji, aż wywołają taką reakcję, na jaką liczyli.

Odchrząknął i zupełnie przyzwoitym angielskim zaczął przedstawiać mi coś, co CIA nazywa *cold pitch* – propozycję współpracy z obcą agencją wywiadowczą. Jest to układ, w którym przedstawiciele obcego kraju nęcą potencjalnego agenta albo źródło obietnicami wyrazów wdzięczności mogącymi przyjmować najróżniejsze postaci – od stosów pieniędzy do immunitetu w wypadku popełnienia dowolnego przestępstwa: poczynając od oszustwa po nawet zabójstwo. Kruczek, rzecz jasna, jest taki, że przedstawiciele obcej agencji zawsze oczekują w zamian czegoś o równej bądź większej wartości. Takie relacje nigdy jednak nie zaczynają się od jednoznacznej propozycji transakcji. W gruncie rzeczy istnieje coś zabawnego w tym, że propozycję tego rodzaju nazywa się *cold*, ponieważ atmosfera, kiedy ląduje na stole, zawsze jest ciepła i pełna udawanej serdeczności, uśmiechów, dowcipów oraz słów współczucia.

Wiedziałem, że muszę wejść mu w słowo. Jeśli nie przerwiesz agentowi obcego wywiadu natychmiast, może nie mieć znaczenia, czy ostatecznie odrzucisz jego ofertę, ponieważ dajesz mu możliwość zniszczenia twojej reputacji, gdyby udostępnił nagranie, jak zastanawiasz się nad jej przyjęciem. I dlatego właśnie, kiedy mężczyzna przepraszał za zamieszanie, wyobraziłem sobie ukryte urządzenia nagrywające i postarałem się starannie dobrać swoje słowa.

– Proszę posłuchać: wiem, kim pan jest i do czego pan zmierza – powiedziałem. – Chcę, żeby było jasne, że nie zamierzam z panem współpracować. Nie będę współpracował z żadną agencją wywiadowczą. Proszę nie poczuć się urażony, ale to nie będzie spotkanie tego rodzaju. Jeśli chce pan przeszukać moją torbę, jest tutaj. – Wskazałem pod krzesło, gdzie leżała. – Ale zapewniam, że nie znajdzie pan w niej niczego, co byłoby panu przydatne.

Gdy mówiłem, twarz mężczyzny przybrała inny wyraz. Zaczął odgrywać urażonego.

– Chyba nie sądzi pan, że zrobilibyśmy coś takiego – stwierdził. – Proszę mi wierzyć, chcemy tylko pomóc.

Sarah odchrząknęła i włączyła się do dyskusji:

– To bardzo uprzejme z pana strony, ale chyba rozumie pan, że zależy nam tylko na tym, by zdążyć na następny lot.

Na ułamek sekundy udawane zatroskanie mężczyzny przemieniło się w irytację.

– Jest pani prawnikiem tego pana?

– Jestem jego doradcą prawnym – odpowiedziała Sarah.

Mężczyzna spytał mnie:

– Zatem przyleciał pan do Rosji, ale nie planuje w niej przebywać?

– Tak.

– Czy mogę w takim razie zapytać, dokąd próbuje się pan dostać? Które miasto jest pańskim celem?

– Quito w Ekwadorze, z przesiadkami w Caracas i Hawanie – odparłem, choć wiedziałem, że zna odpowiedź. Nie było wątpliwości, że ma kopię naszego planu podróży, ponieważ lecieliśmy z Hongkongu Aerofłotem, czyli państwową rosyjską linią lotniczą.

Dotąd obaj czytaliśmy z tego samego scenariusza wywiadowczego, ale nagle rozmowa przybrała nieoczekiwany obrót.

– Nie słyszał pan? – spytał agent. Wstał i spojrzał na mnie tak, jakby przekazywał informację o śmierci członka rodziny. – Obawiam się, że pański paszport jest nieważny.

Byłem tak zaskoczony, że zacząłem się jąkać.

– Przepraszam, ale… ale… nie wierzę.

Mężczyzna nachylił się nad blatem i powiedział:

– Nie, mówię prawdę. Proszę mi wierzyć. To decyzja pańskiego ministra spraw zagranicznych, Johna Kerry’ego. Rząd anulował pański paszport i poinformował linie lotnicze, że nie wolno panu podróżować.

Byłem pewien, że to jakaś sztuczka, ale nie rozumiałem, jaki mogła mieć cel. Sarah wyszarpnęła swój laptop z torby i zaczęła łączyć się z lotniskowym Wi-Fi, zanim zdążyłem powiedzieć:

– Proszę dać nam chwilę.

– Oczywiście, muszą państwo sprawdzić – zgodził się mężczyzna, po czym odwrócił się do swoich współpracowników i zaczął przyjaźnie gawędzić z nimi po rosyjsku, jakby nigdzie mu się nie śpieszyło.

Wszystkie portale, na które zajrzała Sarah, informowały o tym, co od niego usłyszeliśmy. Kiedy rozeszła się wiadomość, że opuściłem Hongkong, Departament Stanu USA ogłosił, że anulował mój paszport.

Unieważnił mi dokument podróży, kiedy byłem jeszcze wysoko w powietrzu.

Nie mogłem w to uwierzyć: mój własny rząd unieruchomił mnie w Rosji. Istniała możliwość, że posunięcie Departamentu Stanu było skutkiem biurokratycznych procedur – kiedy starasz się złapać uciekiniera, rozesłanie listu gończego przez Interpol i anulowanie jego paszportu to standardowa procedura operacyjna. Zastosowanie jej okazało się jednak golem samobójczym, ponieważ dało Rosji ogromne zwycięstwo propagandowe.

– On ma rację – powiedziała Sarah, kręcąc głową.

– Co zamierza pan zrobić? – spytał mężczyzna, przechodząc na naszą stronę stołu.

Zanim zdążyłem wyciągnąć z kieszeni ekwadorski list żelazny, Sarah oznajmiła:

– Bardzo mi przykro, ale muszę doradzić panu Snowdenowi, żeby nie odpowiadał na więcej pytań.

Mężczyzna wycelował we mnie palcem i powiedział:

– Pójdzie pan ze mną.

Wskazał mi gestem dłoni, żebym podążył za nim na koniec sali konferencyjnej, gdzie znajdowało się okno. Trzy albo cztery piętra pod nami znajdowała się ulica, a na niej największy kocioł medialny, jaki kiedykolwiek widziałem, dosłownie setki dziennikarzy uzbrojone w kamery i mikrofony.

Był to imponujący show, możliwe, że zorganizowany przez FSB, a może nie, najprawdopodobniej pół na pół. Prawie wszystko w Rosji jest pół na pół. Teraz przynajmniej wiedziałem, dlaczego Sarah i ja zostaliśmy zaprowadzeni do tej konkretnej salki w tej konkretnej poczekalni.

Wróciłem do swojego fotela, ale nie usiadłem z powrotem.

Mężczyzna odwrócił się od okna, spojrzał mi w oczy i oznajmił:

– Życie osoby w pańskiej sytuacji potrafi być bardzo trudne bez przyjaciół, którzy mogą pomóc. – Pozwolił słowom zawisnąć w powietrzu.

Zaraz je usłyszę, pomyślałem. Bezpośrednie pytanie o informacje.

Mężczyzna powiedział:

– Czy wie pan coś? Zna może jakiś drobiazg, którym mógłby się z nami podzielić?

– Poradzimy sobie sami – odparłem. Sarah podniosła się i stanęła obok mnie.

Mężczyzna westchnął. Odwrócił się i wymamrotał coś po rosyjsku, na co jego kompani wstali i wyszli rządkiem z sali.

– Mam nadzieję, że nie pożałuje pan decyzji – poinformował mnie, po czym ukłonił się delikatnie i również wyszedł. W drzwiach minęło go dwóch urzędników administracji lotniska.

Zażądałem, by pozwolili mi udać się pod bramkę na lot do Hawany, ale udawali, że mnie nie słyszą. Po chwili sięgnąłem do kieszeni i pomachałem im przed nosem listem żelaznym wystawionym przez rząd ekwadorski, ale też go zignorowali.

Spędziliśmy uwięzieni na lotnisku biblijne czterdzieści dni i czterdzieści nocy. W tym czasie złożyłem podanie o azyl polityczny do dwudziestu siedmiu krajów. Ani jeden nie odważył się przeciwstawić presji USA. Niektóre po prostu odmówiły, inne zadeklarowały, że nie będą w stanie rozważyć mojej prośby, dopóki nie znajdę się na ich terytorium – co przekraczało moje możliwości. W ostatecznym rozrachunku jedyną głową państwa, która okazała zrozumienie dla mojej sytuacji, był Burger King – ten ani razu nie odmówił mi whoppera (bez pomidora i cebuli).

Moja obecność na lotnisku szybko stała się globalnym widowiskiem i po pewnym czasie doprowadziła do zdarzenia, które zirytowało Rosjan.

Pierwszego lipca prezydent Boliwii Evo Morales opuszczał Moskwę po udziale w corocznym zebraniu Forum Państw-Eksporterów Gazu (GECF); wyleciał z innego stołecznego portu lotniczego, Wnukowo, w samolocie głowy państwa. Rząd Stanów Zjednoczonych, kierowany podejrzeniami, że znajduję się na pokładzie – ponieważ prezydent Morales składał mi wyrazy solidarności – wywarł nacisk na polityków Włoch, Francji, Hiszpanii i Portugalii, by odmówili maszynie wlotu do ich przestrzeni powietrznej, i skutecznie przekierował ją na lotnisko w Wiedniu. Tam nie udzielono prezydentowi pozwolenia na start, dopóki nie pozwolił przeszukać samolotu, by potwierdzić, że na pokładzie nie ma po mnie śladu. Było to szokujące naruszenie niepodległości, które spotkało się z krytyką ze strony Narodów Zjednoczonych. Incydent stanowił afront wobec Rosji, ukazując, że kraj ten nie potrafi zapewnić głowie innego państwa bezpiecznego powrotu do domu. Udowodnił też Rosjanom i mnie, że każdy lot, wobec którego Stany nabiorą podejrzeń, że stanowi próbę przemycenia mojej osoby, może zostać przekierowany na inne lotnisko i uziemiony.

Zakładam, że w oczach rządu rosyjskiego lepiej było pozbyć się mnie i szaleństwa medialnego, które uniemożliwiało normalne funkcjonowanie najważniejszego lotniska w kraju. Pierwszego sierpnia Rosja udzieliła mi tymczasowego azylu. Sarah i mnie pozwolono opuścić Szeremietiewo, ale ostatecznie tylko jedno z nas poleciało do domu. W tym wspólnym czasie połączyła nas przyjaźń na całe życie. Na zawsze będę jej wdzięczny za tygodnie spędzone u mojego boku, za jej kręgosłup moralny i wytrwałość, którymi się wykazała.

28_Z_dzienników_Lindsay_Mills|

Choć od domu dzieliła mnie wielka odległość, cały czas myślałem o Lindsay. Nie bardzo wiedziałem, jak opowiedzieć historię o niej – o tym, co ją spotkało po mojej ucieczce: o przesłuchaniach FBI, inwigilacji, zainteresowaniu mediów, prześladowaniu online, zagubieniu i cierpieniu, gniewie i smutku. W końcu uświadomiłem sobie, że to sama Lindsay powinna zrelacjonować ten okres. Nikt inny tego nie przeżył, więcej: nikt inny nie ma prawa opisywać tych wspomnień. Na szczęście Lindsay od okresu dojrzewania prowadziła dziennik, gdzie dokumentowała swoje życie i planowała przedsięwzięcia artystyczne. Zgodziła się, żebym zamieścił tu kilkanaście stron jej zapisków. W przedstawionych poniżej fragmentach zmieniono wszystkie imiona (oprócz należących do członków rodziny), poprawiono kilka literówek i dokonano paru zmian redakcyjnych. Poza tym wszystko jest tak, jak było od chwili mojego wyjazdu z Hawajów.

22.05.2013

Zatrzymałam się w K-Marcie, żeby kupić lei. Staram się przywitać Wendy w duchu aloha, ale jestem wkurzona. Ed planuje wizytę matki od tygodni. To on ją zaprosił. Miałam nadzieję, że tam będzie, kiedy obudzę się rano. Podczas jazdy z lotniska do Waipahu Wendy się denerwowała. Nie była przyzwyczajona do jego nagłych wyjazdów. Próbowałam jej wytłumaczyć, że to normalne. Ale to było normalne, kiedy mieszkaliśmy tam, na kontynencie, nie na Hawajach, i nie pamiętałam takiej sytuacji, żeby Ed wyjechał i nie było z nim kontaktu. Poszłyśmy na pyszny obiad, by się

rozerwać, a Wendy mówiła o tym, że jej zdaniem Ed jest na zwolnieniu lekarskim. To bez sensu, jak twierdziła, że kazali mu wyjechać służbowo, skoro wziął wolne z powodów zdrowotnych. Kiedy dotarłyśmy do domu, Wendy natychmiast położyła się do łóżka. Ja sprawdziłam telefon i okazało się, że mam trzy nieodebrane połączenia z nieznanego numeru i jedną z bardzo długiego zagranicznego numeru. Poszukałam go w Google'u. Ed musi być w Hongkongu.

24.05.2013

Wendy na cały dzień została sama w domu i myśli po prostu kłębiły się jej w głowie. Było mi przykro z jej powodu i pocieszała mnie tylko myśl, jak Ed sam radziłby sobie z zabawianiem mojej matki. Przy obiedzie Wendy stale wypytywała mnie o zdrowie Eda, co uznałam za zrozumiałe, skoro sama chorowała na padaczkę. Powiedziała, że się martwi, bo mógł mieć kolejny atak, a potem zaczęła płakać. Po chwili do niej dołączyłam. Właśnie sobie uświadamiam, że ja też się martwię. Ale nie myślę o epilepsji, tylko: a co, jeśli wyjechał, bo ma romans? Kim ona jest? Postaraj się przetrwać tę wizytę i dobrze bawić. Polećcie awionetką na Big Island. Do wulkanu Kilauea, tak jak było zaplanowane. Kiedy Wendy wyjedzie, oceń sytuację na nowo.

3.06.2013

Zawiozłam Wendy na lotnisko, żeby poleciała z powrotem do Marylandu. Nie chciała wracać, ale ma pracę. Odprowadziłam ją tak daleko, jak mogłam pójść, i objęłam. Nie chciałam wypuścić jej z uścisku. Potem stanęła w kolejce do kontroli bezpieczeństwa. Po powrocie do domu zobaczyłam, że status Eda na Skype'ie zmienił się na: „Przepraszam, ale to trzeba było zrobić". Nie wiem, kiedy to zrobił. Mogło to być dzisiaj, ale też

w zeszłym miesiącu. Po prostu sprawdziłam Skype’a i to zauważyłam, ale jestem na tyle szalona, by myśleć, że wysyła mi wiadomość.

7.06.2013

Obudził mnie telefon od agentki specjalnej Megan Smith z NSA, chciała, żebym do niej oddzwoniła w sprawie Eda. Dalej czuję się chora i mam gorączkę. Musiałam zostawić samochód w warsztacie i Tod podrzucił mnie do domu swoim ducatim. Kiedy wjechaliśmy na moją ulicę, zobaczyłam na podjeździe biały rządowy samochód i agentów rozmawiających z sąsiadami. Nigdy nawet nie poznałam swoich sąsiadów. Nie wiem dlaczego, ale w pierwszym odruchu kazałam Todowi jechać dalej. Schyliłam głowę, udając, że szukam czegoś w torebce. Pojechaliśmy do Starbucksa, gdzie Tod pokazał mi w gazecie coś o NSA. Próbowałam przeczytać nagłówki, ale moja paranoja już wyrwała się spod kontroli. Czy dlatego na moim podjeździe był biały SUV? Czy ten sam SUV stoi na parkingu przed Starbucksem? Czy w ogóle powinnam to pisać? Wróciłam do domu i SUV-a już nie było. Łyknęłam lekarstwa i wtedy uświadomiłam sobie, że nic nie jadłam. W środku lunchu zobaczyłam za kuchennym oknem policjantów. Słyszałam przez okno, jak mówią przez radio, że ktoś jest w środku. Ten ktoś to ja. Otworzyłam drzwi frontowe, za którymi stało dwoje agentów i funkcjonariusz HPD*. Byli przerażający. Ten z HPD przeszukiwał dom, w tym czasie agentka Smith wypytywała mnie o Eda, który powinien być z powrotem w pracy 31 maja. Funkcjonariusz HPD powiedział, że to podejrzane, kiedy pracodawca zgłasza czyjeś zaginięcie szybciej niż współmałżonek lub dziewczyna. Patrzył na mnie tak, jakbym zabiła Eda. Rozglądał się po domu w poszukiwaniu jego ciała. Agentka Smith spytała, czy może zobaczyć wszystkie komputery, które mam w domu, i to mnie rozgniewało. Powiedziałam, że jak będzie miała nakaz. Poszli sobie, ale czyhali na rogu.

San Diego, 8.06.2013

Trochę się bałam, że TSA nie pozwoli mi opuścić wyspy. W telewizji na lotnisku pełno było wiadomości o NSA. Kiedy już znalazłam się na pokładzie samolotu, wysłałam e-mail do agentki Smith i detektywa z Wydziału Osób Zaginionych, że moja babcia ma operację na otwartym sercu, więc muszę na kilka tygodni wyjechać z wyspy. Operacja jest zaplanowana na koniec miesiąca i zostanie przeprowadzona we Floridzie, nie w San Diego, ale to wymówka, tylko taką umiałam wymyślić, żeby polecieć na kontynent. Lepsze usprawiedliwienie, niż to, że chcę pobyć z przyjaciółką Sandrą; poza tym są jej urodziny. Kiedy koła samolotu oderwały się od ziemi, zapadłam w pełen ulgi letarg. Po wylądowaniu poczułam, że mam wysoką gorączkę. Z lotniska odebrała mnie Sandra. Nic jej wcześniej nie mówiłam, bo moja paranoja sięgała szczytu, ale sama się domyśliła, że coś się dzieje i że nie odwiedziłam jej tylko ze względu na urodziny. Spytała, czy zerwaliśmy z Edem. Odparłam, że być może.

9.06.2013

Dzwoniła do mnie Tiffany. Spytała, co u mnie, i stwierdziła, że martwi się o mnie. Nie zrozumiałam jej. Przez chwilę milczała. Potem spytała, czy widziałam wiadomości. Powiedziała, że Ed nakręcił wideo i jest na stronie głównej Huffington Posta. Sandra podłączyła laptop do telewizora. W milczeniu czekałam, aż załaduje się dwunastominutowe wideo z YouTube’a. A potem on tam był. Prawdziwy. Żywy. Byłam wstrząśnięta. Wyglądało na to, że schudł, ale brzmiał jak dawny on. Dawny Ed, pewny siebie i silny. Taki, jaki był przed tym ostatnim ciężkim rokiem. To ten mężczyzna, którego pokochałam, a nie ten zimny, zamknięty w sobie duch, z którym ostatnio żyłam. Sandra mnie objęła, a ja nie wiedziałam, co powiedzieć. Stałyśmy w milczeniu. Pojechałyśmy na urodzinowego grilla Sandry do domu jej kuzyna na tym pięknym wzgórzu na południe od

miasta, tuż przy granicy z Meksykiem. Wspaniałe miejsce, ale niewiele do mnie docierało. Zamykałam się w sobie. Nie wiedziałam, jak choćby zacząć oceniać sytuację. Powitały nas przyjazne twarze, ale ludzie nie mieli pojęcia, przez co przechodzę. Ed, co ty narobiłeś? Jak ci się uda z tego wydostać? Myślami byłam daleko od towarzyskich rozmówek na przyjęciu. Mój telefon rozsadzały przychodzące połączenia i SMS-y. Tata. Mama. Wendy. Po grillu wracałam do San Diego za kółkiem durango kuzyna Sandry, bo potrzebowała w tym tygodniu auta do przeprowadzki. Kiedy jechałyśmy, podążał za nami czarny SUV, a wóz policyjny polecił Sandrze zjechać na pobocze – prowadziła samochód, którym ja wcześniej przyjechałam. Nie zatrzymałam się, tylko dalej jechałam durango, mając nadzieję, że trafię do celu, bo mój telefon już padł od tych wszystkich rozmów.

10.06.2013

Wiedziałam, że Eileen** to ważna figura w lokalnej polityce, ale nie miałam pojęcia, że jest też pieprzoną gangsterką. Zajęła się wszystkim. Kiedy czekałyśmy, aż jej kontakty polecą nam prawnika, odebrałam telefon z FBI. Dzwonił agent Chuck Landowski, żeby mnie spytać, co robię w San Diego. Eileen kazała mi się rozłączyć. Zadzwonił ponownie i odebrałam, chociaż Eileen mówiła, że nie powinnam. Agent Chuck powiedział, że nie chciał pojawić się w tym domu niezapowiedziany, więc dzwoni „z czystej grzeczności”, by uprzedzić, że przyjadą agenci. To wyprowadziło Eileen z równowagi. Ona jest taka cholernie twarda, to niesamowite. Kazała mi zostawić telefon w domu, wzięłyśmy jej samochód i jeździłyśmy bez celu, żeby pomyśleć. Do Eileen przyszedł SMS od koleżanki z namiarem na polecanego prawnika, Jerry’ego Fabera. Dała mi telefon i kazała do niego dzwonić. Odebrała sekretarka, której powiedziałam, że nazywam się Lindsay Mills, byłam dziewczyną Edwarda Snowdena i potrzebuję

prawnika. Odparła: „Och, już panią łączę”. Zabawnie było słyszeć w jej głosie, że wie, kim jestem.

Jerry odebrał i spytał, w czym może pomóc. Powiedziałam mu o telefonach z FBI, a on chciał wiedzieć, jak nazywał się dzwoniący agent, żeby móc porozmawiać z federalnymi. Kiedy czekałyśmy, aż Jerry zadzwoni, Eileen zaproponowała, żebyśmy pojechały kupić telefony na kartę, jeden do rozmów z rodziną i przyjaciółmi, a drugi z Jerrym. Po załatwieniu tego Eileen spytała, w jakim banku trzymam pieniądze. Pojechałyśmy do najbliższego oddziału, gdzie kazała mi natychmiast wszystko wypłacić – na wypadek, gdyby federalni chcieli mi zamrozić konta. Weszłam i wybrałam całość oszczędności życiowych w gotówce i czekach bankowych. To Eileen nalegała, żebym tak rozdzieliła środki, i po prostu jej posłuchałam. Dyrektor banku spytał, po co mi tyle gotówki, a ja odparłam: „Na życie”. Miałam ochotę mu powiedzieć: „Gówno ci do tego!”, ale pomyślałam, że jak będę uprzejma, to mnie nie zapamiętają. Martwiłam się, że ludzie zaczną mnie rozpoznawać, bo w wiadomościach stale pokazywali moją twarz obok Eda. Kiedy wyszłyśmy z banku, spytałam Eileen, jak stała się taką ekspertką w postępowaniu w kłopotach. Odparła chłodno: „Jako kobieta musisz wiedzieć takie rzeczy. Na przykład zawsze wypłacasz pieniądze z banku, kiedy się rozwodzisz”. Kupiłyśmy sobie wietnamskie danie na wynos, pojechałyśmy z nim do domu Eileen i zjadłyśmy na podłodze w holu na piętrze. Eileen i Sandra włączyły suszarki do włosów, żeby panował hałas, kiedy szeptem rozmawiałyśmy. Na wypadek, gdyby nas podsłuchiwali.

Potem zadzwonił Jerry i powiedział, że jeszcze dziś musimy spotkać się z FBI. Eileen zawiozła nas do jego kancelarii, a po drodze zauważyła, że nas śledzą. To było bez sensu. Przecież jechałyśmy na rozmowy z federalnymi, tymczasem federalni siedzieli nam na ogonie, dwa SUV-y

i honda accord bez tablic. Eileen przyszło do głowy, że może to nie jest FBI. Być może to jakaś inna agencja albo wywiad zagraniczny i ktoś chce mnie porwać. Zaczęła jechać szybko i nierówno, żeby ich zgubić, ale wszystkie światła zmieniały się na czerwone za każdym razem, kiedy dojeżdżałyśmy do sygnalizatorów. Powiedziałam jej, żeby przestała szaleć i zwolniła. Przy drzwiach budynku Jerry'ego stał agent w cywilnych ciuchach, ale od razu było widać, kim jest. Wjechałyśmy na piętro windą, a kiedy drzwi się otworzyły, zobaczyłyśmy trzech mężczyzn – dwóch z nich okazało się agentami, a trzeci Jerrym. Tylko on uścisnął mi dłoń. Jerry wyjaśnił Eileen, że nie może iść z nami do sali konferencyjnej. Zadzwoni, kiedy skończymy. Ona jednak nalegała, że zaczeka. Usiadła w holu z wyrazem twarzy mówiącym, że może tak czekać nawet milion lat. W drodze Jerry odciągnął mnie na bok i powiedział, że wynegocjował „ograniczony immunitet", ale odparłam, że to w zasadzie nic nie znaczy, a on nie zaprzeczył. Wyjaśnił, że nie wolno mi kłamać, a jeśli nie będę wiedziała, co odpowiedzieć, mam powtarzać, że nie wiem, i pozwolić mówić jemu. Agent Mike miał na twarzy nieco zbyt miły uśmiech, a agent Leland przyglądał mi się, jakbym brała udział w eksperymencie, a on badał moje reakcje. Obaj przyprawiali mnie o dreszcze. Zaczęli od pytań o mnie, tak podstawowych, że wyglądało, jakby chcieli mi udowodnić, że wszystko już o mnie wiedzą. Oczywiście, że wiedzieli. O to właśnie chodziło Edowi. Rząd zawsze wie wszystko. Kazali mi opowiadać o ostatnich dwóch miesiącach, dwa razy, a kiedy skończyłam z tą „osią czasu", agent Mike poprosił, żebym zaczęła wszystko od początku. „Od początku czego?" – spytałam. „Opowiedz mi, jak się poznaliście" – odrzekł.

11.06.2013

Wychodzę z przesłuchania wyczerpana późnym wieczorem, a przede mną jeszcze całe dni kolejnych. Nie powiedzieli mi, ile dokładnie. Eileen

zawiozła nas na spotkanie z Sandrą w jakiejś knajpce, żebyśmy razem zjadły obiad. Po wyjeździe z centrum zauważyłyśmy, że nadal mamy ogony. Eileen znów próbowała go zgubić, przyspieszając i zawracając niezgodnie z przepisami, ale zaczęłam ją błagać, żeby przestała. Pomyślałam, że przez taką jazdę wydam się jeszcze bardziej podejrzana. Ale Eileen jest bardzo uparta i nadopiekuńcza. Na parkingu przed knajpką walnęła w okno jednego ze śledzących nas aut i zaczęła krzyczeć, że przecież ja współpracuję, więc nie ma powodu za mną jeździć. Było to odrobinę żenujące – tak jak sytuacja, kiedy mama wyczekuje na ciebie pod szkołą; ale przede wszystkim ogarnął mnie podziw. Żeby tak podejść do auta z agentami federalnymi i ich zrugać! Sandra siedziała z tyłu lokalu, więc złożyłyśmy zamówienie i rozmawiałyśmy o „obecności w mediach". Byłam we wszystkich wiadomościach.

W połowie obiadu do naszego stolika podeszło dwóch mężczyzn. Jeden wysoki w bejsbolówce i z aparatem ortodontycznym, a drugi ubrany, jakby właśnie wybierał się na clubbing. Wysoki przedstawił się jako agent Chuck, to on wcześniej do mnie dzwonił. Powiedział, że chcą ze mną porozmawiać o „zachowaniu na drodze", kiedy skończymy jeść. W tej chwili uznałyśmy, że już skończyłyśmy. Czekali na mnie przed drzwiami knajpki. Agent Chuck pokazał mi odznakę i wyjaśnił, że jego głównym celem jest zapewnienie mi bezpieczeństwa. Twierdził, że coś może zagrażać mojemu życiu. Poklepał się po marynarce i powiedział, że gdyby zaistniało niebezpieczeństwo, on tym się zajmie, bo jest uzbrojony. Wszystko to było prężeniem muskułów w stylu macho albo próbą zyskania mojego zaufania przez wmawianie mi, że jestem bezbronna. Potem powiedział, że FBI będzie mnie śledzić przez całą dobę, przynajmniej przez najbliższy czas, i taka nieostrożna jazda, jaką prezentowała Eileen, nie będzie tolerowana. Dodał, że agentom nie wolno rozmawiać z obserwowanymi, ale uznał, że

w tych okolicznościach musi „poprowadzić zespół w tym kierunku dla bezpieczeństwa wszystkich”. Dał mi wizytówkę z informacjami kontaktowymi i powiedział, że przez całą noc będzie parkował tuż przed domem Eileen, a ja powinnam do niego dzwonić, jeśli będę potrzebować jego albo czegokolwiek innego. Wyjaśnił też, że wolno mi jeździć wszędzie („no chyba” – pomyślałam), ale kiedy planuję wyjazd, mam mu zawsze wysłać SMS-a. Powiedział: „Otwarta komunikacja wszystko ułatwi”. „Jeśli poinformujesz nas z wyprzedzeniem, będziesz o wiele bezpieczniejsza, obiecuję” – dodał.

16.06.2013–18.06.2013

Przez kilka dni nie pisałam. Jestem taka wściekła, że muszę wziąć głęboki oddech i zastanowić się, na kogo i na co jestem tak zła, bo wszystko mi się zlewa. Pierdoleni federalni! Wyczerpujące przesłuchania, na których traktują mnie, jakbym była winna, i wszędzie za mną jeżdżą, ale, co gorsza, zaburzyli moje zwyczaje. Zazwyczaj szłam sobie do lasu i tam strzelałam lub pisałam, ale teraz wszędzie miałam widownię w postaci śledzących mnie agentów. I to jest tak, jakby zabierając mi energię i czas oraz chęć pisania, odzierali mnie z ostatnich drobin prywatności, które mi jeszcze pozostały. Muszę pamiętać wszystko, co się dzieje. Najpierw kazali mi przynieść laptop i skopiowali twardy dysk. Pewnie przy okazji zamontowali też swoje pluskwy. Potem wydrukowali wszystkie e-maile i chaty, po czym odczytywali, co pisałam do Eda albo on do mnie, i kazali to wyjaśniać. FBI myśli, że wszystko jest szyfrem. Oczywiście że bez kontekstu każda wiadomość wygląda dziwnie. Ale tak porozumiewają się ludzie, którzy byli ze sobą przez osiem lat! Agenci zachowują się, jakby nigdy nie żyli w związku! Zadawali pytania, które miały mnie emocjonalnie wyczerpać, żeby dostać inne odpowiedzi, kiedy wracali do „osi czasu”. Nie przyjmują do wiadomości, że nic nie wiem. W każdym razie stale powracamy do „osi

czasu”, tyle że teraz leżą przed nami zapisy wszystkich moich e-maili i czatów oraz wydruk mojego kalendarza online.

Spodziewałabym się, że agenci rządowi powinni to rozumieć, że Ed zawsze trzymał w tajemnicy swoją pracę, a ja, chcąc z nim być, musiałam to zaakceptować. Ale nie rozumieli. Po pewnym czasie wybuchnęłam płaczem i przesłuchanie skończyło się wcześniej. Agenci Mike i Leland zaproponowali, że odwiozą mnie z powrotem do Eileen, i zanim wyszłam, Jerry wziął mnie na bok i stwierdził, że FBI wydaje się życzliwe. „Chyba cię polubili. Szczególnie Mike”. Przestrzegł mnie też, żebym mimo wszystko była ostrożna w drodze do domu. „Nie odpowiadaj na żadne pytania”. Jak tylko ruszyliśmy, Mike, jakby przy tym był, stwierdził: „Jestem pewien, że Jerry zabronił ci odpowiadać na pytania, ale mam ich tylko kilka”. Jak już się rozgadał, opowiedział mi, że w biurze FBI w San Diego robią zakłady. Najwyraźniej obstawiali, ile czasu zajmie mediom ustalenie mojej lokalizacji. Zwycięzca miał dostać darmowe martini. Później Sandra wyraziła wątpliwości. „Jak znam facetów – stwierdziła – zakładają się o coś innego”.

19.6.2013–20.6.2013

Podczas gdy reszta kraju stara się uporać ze świadomością, że naruszana jest ich prywatność, ja jestem z niej odzierana w zupełnie innym wymiarze. A wszystko to przez Eda. Nienawidzę wysyłać Chuckowi „informacji o wyjazdach”, a potem nienawidzę siebie, że nie miałam odwagi, by tego nie zrobić. Najgorzej było wtedy, gdy powiadomiłam, że jadę spotkać się z Sandrą, i po drodze zabłądziłam, ale nie chciałam prosić śledzących mnie agentów o pomoc i w rezultacie ciągnęłam ich za sobą, zataczając kręgi. Pomyślałam, że może założyli w aucie Eileen podsłuch, więc zaczęłam głośno mówić z myślą, że może mnie słyszą. Właściwie nie tyle mówiłam, co ich przeklinałam. Musiałam pojechać zapłacić Jerry’emu i kiedy już to

zrobiłam, potrafiłam myśleć tylko o marnowaniu pieniędzy podatników na jeżdżenie za mną do prawnika i na siłownię. Po dwóch pierwszych dniach spotkań nie miałam co na siebie włożyć, więc pojechałam do Macy's. Agenci podążyli za mną nawet do działu damskiego. Zastanawiałam się, czy zamierzają wejść również do przymierzalni i komentować, że to wygląda dobrze, tamto źle, a w zielonym mi nie do twarzy. Przy wejściu do przymierzalni wisiał telewizor, właśnie z rykiem leciały wiadomości i zamarłam, kiedy prezenter oznajmił „Dziewczyna Edwarda Snowdena". Wybiegłam z kabiny i stanęłam przed ekranem. Patrząc, jak pokazują moje zdjęcia, wyszarpnęłam z kieszeni telefon i popełniłam ten błąd, że wyszukałam siebie w Google'u. Tyle komentarzy nazywających mnie striptizerką i dziwką. Ale to nie ja. Oni, tak samo jak federalni, już zdecydowali, kim jestem.

22.06.2013–24.06.2013

Przesłuchania się skończyły, przynajmniej na razie. Ale nadal mam ogon. Wyszłam z domu szczęśliwa, że znów znajdę się w powietrzu w miejscowym klubie akrobatyki na szarfach. Pojechałam do klubu i nie mogłam znaleźć miejsca do zaparkowania, ale mojemu ogonowi się udało. Musiał jednak je opuścić, bo wyjechałam poza zasięg śledzących. Wtedy zawróciłam i ukradłam im miejsce. Rozmawiałam przez telefon z Wendy i obie stwierdziłyśmy, że choć Ed tak bardzo nas zranił, to dobrze zrobił, że postarał się, byśmy były razem, gdy wyjechał. To dlatego ją zaprosił i tak bardzo się upierał na jej przyjazd. Chciał, żebyśmy były razem na Hawajach, kiedy wszystko wyjdzie na jaw, oraz dotrzymywały sobie towarzystwa, wspierały się nawzajem i pocieszały. Tak trudno być złym na kogoś, kogo kochasz. A jeszcze trudniej na osobę, którą kochasz i szanujesz za to, że postąpiła właściwie. Obie z Wendy zalałyśmy się łzami, a potem zamilkłyśmy. Sądzę, że w jednej chwili pomyślałyśmy to samo. Jak

możemy rozmawiać jak normalni ludzie, kiedy oni podsłuchują wszystkie nasze rozmowy?

25.06.28013

Z Los Angeles do Honolulu. W miedzianej peruce w drodze na samolot, przez kontrolę bezpieczeństwa i cały rejs. Sandra jechała ze mną. Przed lotem zjadłyśmy ohydny lunch na lotnisku. Kolejne telewizory włączone na CNN nadal pokazywały Eda, i choć dla mnie to surrealistyczne, dla pozostałych realistyczne. Nowa rzeczywistość. Dostałam SMS-a od agenta Mike'a, żebyśmy z Sandrą spotkały się z nim przy bramce 73. Coś podobnego! Przyjechał do Los Angeles z San Diego? Bramka 73 była oddzielona liną i pusta. Mike czekał na nas, siedząc na jednym z krzesełek w rzędzie. Miał skrzyżowane nogi, tak że demonstrował przymocowany do kostki pistolet. Znów idiotyczne męskie zastraszanie. Miał dla mnie papiery do podpisania, żeby FBI wydało mi kluczyki do samochodu Eda w Honolulu. Powiedział, że dwóch agentów będzie na nas czekać tam z kluczem. Inni polecą z nami. Przeprosił, że on osobiście nie leci. Bleee.

29.6.2013

Likwiduję dom już od kilku dni z małymi przerwami, gdy FBI przywozi kolejne papiery do podpisania. Jaka to tortura przeglądać to wszystko. Natykać się na te wszystkie drobiazgi, które mi o nim przypominają. Zachowuję się jak wariatka, sprzątam, a potem nagle wlepiam wzrok w jego połowę łóżka. Częściej jednak odkrywam, czego brakuje. Co zabrało FBI. Nie tylko całą elektronikę, ale i książki. Agenci zostawili ślady butów, rysy na ścianach i kurz.

30.06.2013

Wyprzedaż rzeczy używanych w Waipahu. Na ogłoszenie Sandry – „Zabrać wszystko, najlepsza oferta” – odpowiedziało trzech mężczyzn na craiglist. Przyjechali, żeby grzebać w życiu Eda. Wzięli fortepian, gitarę, zestaw ciężarków. Wszystko, z czym nie mogłam żyć lub nie stać mnie było, by wysłać to na kontynent. Mężczyźni załadowali pikapa po brzegi, a po pewnym czasie wrócili po kolejną partię. Ku mojemu zaskoczeniu, a myślę, że i Sandry, nie za bardzo mi przeszkadzało, że buszują po domu. Ale kiedy odjechali ten drugi raz, porzygałam się.

2.07.2013

Wysłałyśmy dziś prawie wszystko, poza futonami i kanapą, których właśnie się pozbywam. Rzeczy Eda pozostałe po najeździe FBI na dom zmieściły się w niewielkim kartonowym pudełku. Trochę zdjęć i ubrań, mnóstwo skarpetek nie do pary. Żadne dowody dla sądu, tylko po prostu dowody naszego wspólnego życia. Sandra przyniosła benzynę do zapalniczek i przeniosła metalowy kosz na śmieci na lanai na tyły domu. Wrzuciłam wszystkie rzeczy Eda, zdjęcia i ubrania, do środka, zapaliłam opakowanie zapałki i wrzuciłam na wierzch. Siedziałyśmy, patrząc, jak to wszystko się pali, a dym unosi ku niebu. Blask ognia i dym przypomniały mi o wycieczce, jaką odbyłam z Wendy do wulkanu Kilauea na Big Island. To było zaledwie miesiąc temu, a miałam wrażenie, jakby minęły całe lata. Skąd mogłyśmy wiedzieć, że nasze życie za chwilę wybuchnie? Że wulkan Ed zamierza wszystko zniszczyć? Ale pamiętam też, że przewodnik na Kilauea tłumaczył, że wulkany są destrukcyjne, tylko jeśli patrzymy na nie z krótkiej perspektywy. Długofalowo ich działalność jest korzystna dla świata. Tworzą wyspy, schładzają planetę i wzbogacają glebę. Lawa wypływa z nich w niekontrolowany sposób, ale potem schładza się i twardnieje. Popiół, który wyrzucają w powietrze, opada jako sole mineralne, a te użyźniają ziemię i wspomagają wzrost nowego życia.

* HPD, Hawai’i Police Department – Policja Hawajów.

** Matka Sandry.

29_Miłość_i_banicja|

Jeśli podczas lektury tej książki jakiś termin zaintrygował cię na tyle, że postanowiłeś dowiedzieć się czegoś więcej i wpisałeś go do wyszukiwarki – i jeśli było to słowo w rodzaju XKEYSCORE, czyli takie, które może wzbudzić pewne podejrzenia – to gratuluję. Padłeś ofiarą własnej ciekawości i zostałeś wciągnięty do systemu.

Nawet jeśli nie szukałeś żadnych dodatkowych informacji w internecie, to rząd i tak może z łatwością dowiedzieć się o tym, że czytałeś tę książkę. A przynajmniej jest w stanie bez trudu ustalić, że posiadasz jej kopię niezależnie od tego, czy jest to wersja elektroniczna pobrana nielegalnie z sieci, czy wersja papierowa kupiona w sklepie internetowym albo w tradycyjnej księgarni przy użyciu karty kredytowej.

Chciałeś po prostu otworzyć książkę i oddać się lekturze – tym samym wziąć udział w jednym z najbardziej intymnych ludzkich doświadczeń, jakim jest spotkanie umysłów za pośrednictwem języka. Ale to wystarczyło. Twoje naturalne pragnienie nawiązania kontaktu ze światem zostało wykorzystane do skojarzenia twojej osoby z szeregiem unikalnych identyfikatorów: twoim adresem e-mail, numerem telefonu i adresem IP twojego komputera. Poprzez stworzenie systemu obejmującego zasięgiem cały świat i pozwalającego śledzić wspomniane wyżej identyfikatory we wszystkich możliwych kanałach komunikacji elektronicznej amerykańska Wspólnota Wywiadów zyskała możliwość zapisywania oraz przechowywania przez nieograniczony czas danych z twojego życia.

A to był dopiero początek. Kiedy amerykańskie agencje wywiadowcze przekonały się, że możliwe jest pasywne zbieranie wszystkich danych, jakie otrzymujesz i przekazujesz za pośrednictwem elektronicznych środków komunikacji, zaczęły eksperymentować z aktywnymi metodami inwigilowania urządzeń telekomunikacyjnych. Szpikując przesyłane na twoje urządzenia wiadomości fragmentami złośliwego kodu, tak zwanymi exploitami, uzyskały dostęp nie tylko do twoich słów. Obecnie potrafią przejąć zdalnie pełną kontrolę nad twoim sprzętem elektronicznym, w tym także nad wbudowanymi kamerami i mikrofonami. Oznacza to, że jeśli czytasz teraz to zdanie na nowoczesnym urządzeniu, na przykład na tablecie albo smartfonie, to specjaliści z rządowych agencji mogą równocześnie „czytać ciebie”. Są w stanie sprawdzić, jak szybko przewracasz strony i czy czytasz tę książkę od deski do deski, czy przeskakujesz między rozdziałami. Jeśli może im to pomóc w zdobyciu potrzebnych informacji i ustaleniu twojej tożsamości, gotowi są zaglądać ci w nozdrza i obserwować, jak w trakcie lektury bezgłośnie poruszasz ustami.

Oto skutek dwóch dekad niekontrolowanego postępu technicznego, efekt poczynań kasty polityków i specjalistów z dziedziny najnowszych technologii, która rości sobie prawo do bycia twoim nadzorcą. Nieważne, gdzie przebywasz i co robisz – twoje życie stało się otwartą księgą.

Ponieważ masowa inwigilacja z samej definicji jest stale obecna w naszym codziennym życiu, doszedłem do wniosku, że powinniśmy być nieustannie świadomi stwarzanych przez nią zagrożeń, a także szkód, jakie zdążyła już wyrządzić. Przekazując zebrane przeze mnie informacje dziennikarzom, chciałem obnażyć system i upewnić się, że nie będzie ignorowany w moim kraju ani za granicą. Po roku 2013 świadomość masowej inwigilacji systematycznie rośnie: coraz więcej osób zdaje sobie sprawę z problemu,

a także coraz lepiej rozumie, na czym on polega. Ale w dobie mediów społecznościowych musimy też nieustannie pamiętać o tym, że sama świadomość to zbyt mało.

W Stanach Zjednoczonych pierwsze prasowe doniesienia na temat ujawnionych przeze mnie informacji zapoczątkowały, jak ujął to prezydent Obama, „ogólnonarodową debatę". Doceniałem te słowa, ale żałowałem, że głowa państwa nie wspomniała o tym, że zarówno sama debata, jak i jej ogólnonarodowy charakter stały się możliwe dzięki temu, że amerykańska opinia publiczna po raz pierwszy została na tyle dobrze poinformowana, by mogła zabrać w tej sprawie głos.

Rewelacje, które wyszły na jaw w 2013 roku, wywołały szczególne poruszenie w Kongresie Stanów Zjednoczonych. Senat oraz Izba Reprezentantów powołały komisje śledcze mające zbadać nadużycia NSA. Dochodzenia wykazały niezbicie, że NSA wielokrotnie okłamywała kongresmenów – i to nawet tych, którzy byli członkami komisji do spraw wywiadu i posiadali najwyższe możliwe poświadczenia bezpieczeństwa – co do charakteru oraz efektów masowej inwigilacji.

W 2015 roku federalny sąd apelacyjny wydał wyrok w sprawie ACLU* kontra Clapper; jej przedmiotem była kwestia legalności prowadzonego przez NSA programu zbierania danych dotyczących połączeń telefonicznych. Sąd orzekł, że program NSA stanowił pogwałcenie nawet tych luźnych wymogów, jakie nałożyła na amerykańskie służby wywiadowcze ustawa patriotyczna (Patriot Act); co więcej, zdaniem sądu działania NSA nosiły znamiona niekonstytucyjnych. W uzasadnieniu wyroku skupiono się na stosowanej przez NSA interpretacji paragrafu 215 Patriot Act, który przyznawał rządowym agencjom prawo do uzyskania od strony trzeciej dostępu do „wszelkich materiałów", jakie agencja uzna za „istotne" dla dochodzeń prowadzonych w sprawach związanych

z aktywnością obcych służb wywiadowczych lub z działalnością terrorystyczną. W opinii sądu rządowa definicja „istotności” była tak szeroka, że faktycznie pozbawiała to pojęcie znaczenia. Określanie niektórych gromadzonych danych mianem „istotnych” tylko dlatego, że mogły okazać się istotne w jakiejś bliżej nieokreślonej przyszłości, uznane zostało za „bezprecedensowe i bezzasadne”. Odmowa przyjęcia przez sąd federalny rządowej definicji skłoniła wielu prawników do uznania wyroku w procesie ACLU kontra Clapper za podważenie prawomocności wszystkich rządowych programów masowego gromadzenia danych, bazujących na doktrynie przyszłej istotności. W następstwie orzeczenia federalnego sądu apelacyjnego Kongres uchwalił ustawę wolnościową (Freedom Act), która wprowadzała poprawki do paragrafu 215 ustawy patriotycznej, zakazujące amerykańskiemu rządowi masowego gromadzenia danych o rozmowach telefonicznych obywateli Stanów Zjednoczonych. Dane te miały pozostawać pod wyłączną kontrolą operatorów telekomunikacyjnych – chcąc uzyskać do nich dostęp, agencje rządowe musiały odtąd w konkretnych przypadkach złożyć formalny wniosek i poparty zgodą wyrażoną przez FISC (Foreign Intelligence Surveillance Court), czyli specjalny sąd zajmujący się sprawami związanymi z działalnością kontrwywiadowczą.

Wyrok w sprawie ACLU kontra Clapper był niewątpliwie ważnym zwycięstwem obrońców wolności obywatelskich. Ustanowiony został znaczący precedens. Uznano mianowicie prawo obywateli Stanów Zjednoczonych do sądowego sprzeciwu wobec tajnych rządowych programów masowej inwigilacji. Po upublicznieniu informacji na temat inwigilacyjnych praktyk agencji rządowych na wokandę trafił cały szereg podobnych spraw. Fakt, że wiele z nich toczy się nadal i każda taka kwestia wiąże się z koniecznością toczenia długich sądowych batalii, utwierdził

mnie w przekonaniu, że wykorzystanie środków prawnych w roli narzędzia sprzeciwu wobec masowej inwigilacji to dopiero faza wstępna działań, które powinny stać się globalnym ruchem oporu wobec poczynań zarówno instytucji państwowych, jak i sektora prywatnego.

Informacje o nadużyciach NSA wywołały także szybką i zdecydowaną reakcję technokapitalistów; po raz kolejny okazało się, że w obliczu wyjątkowego zagrożenia zawiązują się zupełnie nieoczekiwane sojusze. Z ujawnionych dokumentów wynikało, że NSA była do tego stopnia zdeterminowana, by pozyskiwać dane, które uważała za celowo przed nią ukrywane, że podejmowała mnóstwo działań mających na celu osłabienie podstawowych sieciowych protokołów szyfrujących. W rezultacie zwiększyło się ryzyko wycieku poufnych informacji amerykańskich obywateli, na przykład dokumentacji medycznej czy finansowej. Miało to negatywne konsekwencje dla przedsiębiorstw z branży nowoczesnych technologii, ponieważ narażało te podmioty na utratę zaufania klientów, którzy powierzali im swoje wrażliwe dane. W odpowiedzi na doniesienia o praktykach NSA firma Apple wprowadziła nowe, silniejsze domyślne mechanizmy szyfrujące w iPhone’ach oraz iPadach; podobnie postąpił Google, wprowadzając nowe zabezpieczenia w urządzeniach z systemem operacyjnym Andriod, a także w Chromebookach. Ale najważniejszą zmianą w kwestii ochrony prywatności, jaka dokonała się w sektorze prywatnym, było zjawisko masowego przechodzenia właścicieli stron internetowych z protokołu http (Hypertext Transfer Protocol) na szyfrowaną wersję https („s” od *security* – bezpieczeństwo), co pozwoliło znacząco zmniejszyć ryzyko przechwytywania przesyłanych w internecie danych. Przełomowy pod tym względem okazał się rok 2016, kiedy po raz pierwszy od powstania internetu ilość połączeń szyfrowanych była większa od ilości połączeń nieszyfrowanych.

Nie ulega wątpliwości, że internet jest dziś bezpieczniejszy niż w roku 2013. Wynika to zwłaszcza z rosnącej na całym świecie świadomości, że trzeba stosować aplikacje i narzędzia szyfrujące. Ja sam zaangażowałem się w projektowanie i tworzenie kilku takich aplikacji w ramach pracy w zarządzie Fundacji na rzecz Wolności Prasy (Freedom of the Press Foundation, FPF) – organizacji non profit wspierającej dziennikarstwo w interesie publicznym. Znaczna część zadań tej fundacji polega na ochronie praw wynikających z pierwszej i czwartej poprawki do konstytucji Stanów Zjednoczonych poprzez rozwijanie technologii szyfrowania danych. FPF wspiera finansowo Open Whisper Systems, twórców niekomercyjnej aplikacji Signal, czyli szyfrowanej platformy komunikacyjnej, umożliwiającej wysyłanie wiadomości tekstowych oraz wykonywanie połączeń głosowych; FPF rozwija także projekt SecureDrop, bazujący na kodzie źródłowym napisanym przez nieżyjącego już Aarona Swartza. SecureDrop to system pozwalający demaskatorom i innym źródłom informacji na bezpieczne i anonimowe przekazywanie dokumentów mediom. Obecnie SecureDrop dostępny jest w dziesięciu wersjach językowych; korzysta z niego ponad siedemdziesiąt redakcji i agencji informacyjnych, w tym „New York Times”, „Washington Post”, „Guardian” czy „New Yorker”.

W idealnym, a więc nieistniejącym świecie sprawiedliwe prawo czyniłoby takie narzędzia zbędnymi. Ale w świecie, w którym przyszło nam żyć, są one dziś potrzebne bardziej niż kiedykolwiek wcześniej. Zmiana prawa jest nieporównanie trudniejsza od modyfikacji technicznych standardów; tak długo jak regulacje prawne nie będą nadążały za postępem technologicznym, rozmaite instytucje będą próbowały wykorzystać tę sytuację do realizacji własnych celów. Rolą niezależnych twórców sprzętu i otwartego oprogramowania jest likwidowanie luki między prawem

a techniką poprzez zapewnianie odpowiednich narzędzi do ochrony podstawowych swobód obywatelskich, których prawo nie chce lub nie jest w stanie chronić.

Moja obecna sytuacja nieustannie przypomina mi o tym, że o ile przepisy prawne są specyficzne dla danego kraju, o tyle technologia wszędzie jest jednakowa. Każde państwo ma swoje własne kodeksy, ale we wszędzie korzysta się z tego samego kodu komputerowego. Technologia z łatwością przekracza granice i jest obywatelką świata. Z upływem czasu staje się dla mnie coraz bardziej oczywiste, że reformowanie ustaw w celu zmiany polityki inwigilacyjnej w kraju mojego urodzenia nie pomoże w niczym dziennikarzowi czy dysydentowi w kraju mojego wygnania. Pomóc im może smartfon z oprogramowaniem do szyfrowania danych.

W perspektywie międzynarodowej ujawnione przeze mnie dokumenty i informacje przyczyniły się do ożywienia debaty na temat szpiegowania w krajach o długiej historii nadużyć popełnianych przez władze. Przeciwko amerykańskiej polityce masowej inwigilacji najgłośniej protestowali obywatele tych państw, których rządy najbliżej współpracowały z władzą Stanów Zjednoczonych – było tak w przypadku członków Sojuszu Pięciorga Oczu (przede wszystkim Wielkiej Brytanii; brytyjska służba specjalna – Centrala Łączności Radiowej – do dziś pozostaje głównym zagranicznym partnerem NSA), a także krajów członkowskich Unii Europejskiej. Niemcy, które w przeszłości zrobiły bardzo wiele, by rozliczyć się ze swoją nazistowską i komunistyczną historią, stanowią najlepszy przykład rozbieżności między opinią społeczeństwa a postępowaniem władzy. Niemieccy obywatele byli zbulwersowani na wieść, że NSA masowo gromadziła dane dotyczące komunikacji elektronicznej oraz połączeń telefonicznych wykonywanych na terenie

Niemiec, a nawet posunęła się do podsłuchiwania smartfonu kanclerz Angeli Merkel. W tym samym czasie niemiecka agencja wywiadowcza BND prowadziła wspólnie z NSA wiele różnych operacji oraz realizowała dla amerykańskich partnerów zadania, których NSA z różnych względów nie mogła lub nie chciała wykonać.

Niemal każdy kraj na świecie stanął przed podobnym dylematem: obywatele kipieli oburzeniem na praktyki, w jakie zamieszane były ich władze. Demokratycznie wybrany rząd, który inwigiluje własnych obywateli uważających takie działania za sprzeczne z demokratycznymi zasadami przestaje być *de facto* rządem demokratycznym. Ten kognitywny dysonans przyczynił się do wprowadzenia do międzynarodowego dyskursu o prawach człowieka kwestii prywatności.

Po raz pierwszy od zakończenia II wojny światowej rządy państw o ustroju liberalno-demokratycznym zaczęły uznawać prywatność za naturalne, przyrodzone prawo każdego mężczyzny, każdej kobiety i każdego dziecka. Nawiązywano przy tym do Powszechnej Deklaracji Praw Człowieka, uchwalonej w 1948 roku przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych. Artykuł 12 tego dokumentu stanowi: „Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu”. Postanowienia artykułu 12, podobnie jak wiele rezolucji i deklaracji ONZ, nigdy nie były egzekwowane; pozostały na papierze wyrazem niezrealizowanych marzeń o zagwarantowaniu swobód obywatelskich wszystkim mieszkańcom świata, którzy dopiero co doświadczyli koszmaru ludobójstwa i broni nuklearnej oraz mierzyli się ze zjawiskiem przesiedleń i migracji na niespotykaną wcześniej skalę.

Unia Europejska, wciąż kultywująca dziedzictwo tego powojennego uniwersalistycznego idealizmu, jako pierwsza organizacja o charakterze międzynarodowym podjęła próbę wprowadzenia w życie zasad sformułowanych w artykule 12 Powszechnej Deklaracji Praw Człowieka. Przyjęła nową dyrektywę o ochronie osób zgłaszających przypadki naruszenia prawa w krajach członkowskich Wspólnoty, a także wprowadziła ujednolicone ramy prawne dotyczące ochrony prywatności. W roku 2016 europejski parlament uchwalił tak zwane ogólne rozporządzanie o ochronie danych, nazywane też rozporządzeniem o ochronie danych osobowych (w skrócie RODO) – najważniejszą jak dotąd próbę powstrzymania narastającej hegemonii nowoczesnej technologii w Unii Europejskiej uważanej, niebezpodstawnie zresztą, za przedłużenie politycznej dominacji Stanów Zjednoczonych.

RODO uznaje obywateli krajów Unii Europejskiej, określanych mianem „osób fizycznych”, za „podmioty danych” – czyli za osoby generujące dane osobowe i możliwe do zidentyfikowania na podstawie danych osobowych. W Stanach Zjednoczonych dane uważane są w większości przypadków za własność tego, kto je przechowuje. W Unii Europejskiej uznaje się je za należące do tego, kogo dotyczą; dzięki temu nasza podmiotowość posiadacza danych osobowych zasługuje na ochronę wynikającą z wolności obywatelskich.

RODO to bez wątpienia istotny prawny krok naprzód, ale ponadnarodowy charakter tych przepisów jest wciąż zbyt wąski: internet jest bowiem zjawiskiem globalnym. Nasza osobowość fizyczna nigdy nie będzie równoznaczna pod względem prawnym z naszą podmiotowością posiadaczy danych osobowych, chociażby z uwagi na to, że fizycznie możemy przebywać tylko w jednym miejscu w danym czasie, natomiast nasze dane osobowe znajdują się w wielu miejscach równocześnie.

Dzisiaj niezależnie od tego, kim i gdzie jesteśmy – gdzie przebywa nasze fizyczne ja – znajdujemy się jednocześnie w wielu innych miejscach, daleko poza granicami własnego kraju. Cząstki naszego jestestwa błąkają się po łączach internetu, bezdomne, a zarazem podlegające prawu każdego państwa, do którego zawędrują. Informacje na temat mojego pobytu w Genewie znajdują się w Beltway. Zdjęcia z uroczystości ślubnej wykonane w Tokio są w Sydney. Zapisane w iCloud filmy z ceremonii pogrzebowej w Waranasi mieszczą się częściowo w centrum danych Apple'a w Karolinie Północnej, moim rodzinnym stanie, a po części rozsiane są po partnerskich serwerach firm Amazon, Google, Microsoft i Oracle w Unii Europejskiej, Wielkiej Brytanii, Korei Południowej, Singapurze, na Tajwanie i w Chinach.

Nasze dane nieustannie migrują, trafiając do najodleglejszych zakątków świata.

Zaczynamy generować informacje, zanim jeszcze przyjdziemy na świat – kiedy sprzęt medyczny wykrywa naszą obecność w łonie matki; dane o nas będą też rozprzestrzeniać się nawet po naszej śmierci. Świadomie tworzone wspomnienia, czyli dane dokumentujące rozmaite fakty i wydarzenia, które decydujemy się zatrzymać, stanowią oczywiście jedynie drobny ułamek informacji na temat naszego życia, pozyskiwanych i gromadzonych – w większości wypadków bez naszej wiedzy lub zgody – przez inwigilujące nas instytucje prywatne i rządowe. Jesteśmy pierwszymi ludźmi w dziejach świata dotkniętymi problemem nieśmiertelności danych; jako pierwsi musimy zmierzyć się z prawdą, że informacje na nasz temat mogą istnieć wiecznie. To dlatego spoczywa na nas szczególna powinność. Musimy zadbać o to, by dane o naszej przeszłości nie zostały wykorzystane przeciwko nam ani naszym dzieciom.

W obronie wolności, jaką jest prywatność, staje obecnie nowe pokolenie. Osoby urodzone po 11 września 2001 roku przez całe dotychczasowe życie poddane były wszechobecnej inwigilacji. Ci młodzi ludzie, którzy nie mieli okazji poznać innego świata, postanowili go sobie wyobrazić – ich społeczna i polityczna kreatywność oraz techniczna pomysłowość napełniają mnie nadzieją.

Jeśli jednak nie odzyskamy teraz kontroli nad należącymi do nas danymi, to nasze dzieci mogą już nie być w stanie tego zrobić. Zarówno one, jak i ich potomkowie znajdą się w pułapce – przedstawiciele każdej kolejnej generacji będą zmuszeni dźwigać brzemię w postaci ogromnych ilości danych osobowych przodków; kolejne pokolenia poddane będą programom masowego gromadzenia informacji, których potencjał kontrolowania i manipulowania społeczeństwem wykraczać będzie daleko nie tylko poza ramy prawa, ale i poza granice wyobraźni.

Kto z nas potrafi przewidzieć przyszłość? Kto ośmieliłby się to zrobić? Odpowiedź na pierwsze pytanie brzmi: nikt. Odpowiedź na drugie: wszyscy, a zwłaszcza każdy rząd i każda firma. Do tego właśnie wykorzystywane są nasze dane. Algorytmy analizują je w poszukiwaniu wzorców zachowań, na których podstawie przewidują nasze przyszłe zachowania – jest to rodzaj cyfrowego proroctwa, niewiele bardziej trafnego niż wróżenie z ręki. Jeśli przyjrzysz się bliżej mechanizmom leżącym u podstaw tych przewidywań, dojdziesz do wniosku, że ich naukowa podbudowa jest w rzeczywistości antynaukowa i to, co rzekomo ma być przewidywaniem, tak naprawdę jest manipulacją. Kiedy strona internetowa podpowiada ci, że skoro spodobała ci się moja książka, to możesz docenić również książki Jamesa Clappera czy Michaela Haydena, to masz do czynienia nie tyle z opartą na racjonalnych przesłankach hipotezą, co raczej z subtelną formą przymusu.

Nie możemy dawać się tak wykorzystywać. Nie możemy godzić się na to, by wykorzystywano nasze dane do sprzedawania nam rzeczy, które nie powinny być na sprzedaż, na przykład publicystyki. Jeśli na to przystaniemy, będziemy otrzymywać jedynie takie opinie, na jakich nam zależy, albo takie, jakie chcą nam przekazać możni tego świata – zamiast prawdziwej publicystyki polegającej na szczerej wymianie poglądów. Nie możemy pozwolić, by wszechwładne i wszechobecne programy inwigilacyjne były wykorzystywane do „obliczania" naszego wyniku w systemie punktacji obywateli albo do „przewidywania" naszych przestępczych działań; do mówienia, czy mamy prawo się kształcić lub pracować; do dyskryminacji na podstawie naszej przeszłości prawnej, finansowej czy zdrowotnej, a także rasy czy przynależności etnicznej. Jeśli zaś chodzi o najbardziej osobiste dane, czyli o informacje genetyczne, to jeśli zgodzimy się, by wykorzystywano je w celach identyfikacyjnych, prędzej czy później zostaną użyte do tego, by nas represjonować, a nawet zmieniać – przekształcać istotę człowieczeństwa na obraz i podobieństwo technologii, która dąży do poddania nas swojej kontroli.

Oczywiście wszystko to już się dzieje.

Banicja: od 1 sierpnia 2013 roku codziennie przypominam sobie o tym, że jako nastolatek nazywałem „banicją" brak dostępu do internetu. Problem z Wi-Fi? Banicja. Brak zasięgu? Banicja. Kilkunastoletni chłopak, który używał tego określenia, wydaje mi się teraz taki młody. I tak bardzo odległy.

Kiedy ludzie pytają mnie, jak obecnie żyję, odpowiadam, że podobnie do nich; tak samo jak oni spędzam mnóstwo czasu przed komputerem – czytam, piszę i komunikuję się z innymi. Z„nieujawnionego miejsca pobytu", jak zwykła pisać prasa, a tak naprawdę z wynajmowanego przeze

mnie trzypokojowego mieszkania w Moskwie łączę się z uczestnikami rozmaitych sympozjów i konferencji na całym świecie. Pojawiam się na ustawionym na scenie ekranie, żeby opowiadać studentom, naukowcom, prawodawcom i specjalistom z dziedziny nowych technologii o ochronie swobód obywatelskich w erze cyfrowej.

Czasem odbywam też wirtualne narady z pozostałymi członkami zarządu Fundacji na rzecz Wolności Prasy albo dyskutuję ze sztabem moich europejskich prawników pod kierownictwem Wolfganga Kalecka z Europejskiego Centrum Praw Konstytucyjnych i Praw Człowieka. Kiedy indziej kupuję coś na wynos w Burger Kingu – nie zapomniałem, skąd pochodzę – i gram w gry komputerowe; jestem zdany na pirackie kopie, ponieważ nie mogę posługiwać się kartami kredytowymi. Stałym punktem każdego dnia jest pogawędka z moim amerykańskim adwokatem, powiernikiem i doradcą, Benem Wiznerem z ACLU. Ben pełni rolę mojego przewodnika po świecie takim, jakim on jest, a także cierpliwie wysłuchuje moich przemyśleń na temat tego, jaki świat być powinien.

Tak właśnie wygląda moje życie. Zmieniło się ono na lepsze mroźnej zimy 2014 roku, kiedy przyjechała do mnie Lindsay. Miało to być nasze pierwsze spotkanie odkąd, opuściłem Hawaje. Starałem się nie obiecywać sobie zbyt wiele po jej wizycie, bo wiedziałem, że nie zasługuję na to, by dała mi drugą szansę – należał mi się raczej siarczysty policzek. Ale kiedy otworzyłem drzwi, Lindsay położyła dłoń na mojej twarzy, a ja powiedziałem jej, że ją kocham.

– Ciii… – odparła. – Wiem.

Trzymaliśmy się w objęciach, a każdy nasz oddech składał obietnicę nadrobienia straconego czasu.

Od tamtej chwili mój świat stał się jej światem. Wcześniej najchętniej spędzałem czas w domu – podobnie było, zanim jeszcze znalazłem się

w Rosji – ale Lindsay, dla której była to pierwsza wizyta w Moskwie, nalegała na wspólne zwiedzanie miasta.

Rosyjski prawnik, Anatolij Kuczerena, który pomógł mi uzyskać azyl w Rosji – jako jedyny okazał się na tyle przewidujący, by pojawić się na lotnisku w towarzystwie tłumacza – to bardzo kulturalny i zaradny człowiek. Potrafi nie tylko znakomicie radzić sobie z wszelkimi prawnymi zawiłościami, ale także zdobyć na ostatnią chwilę bilety do opery. Po przyjeździe Lindsay załatwił nam dwa miejsca w loży teatru Bolszoj. Wystroiliśmy się więc i wybraliśmy na wieczorny spektakl, chociaż muszę przyznać, że byłem pełen obaw. W foyer panował ścisk, kłębiło się mnóstwo ludzi. Lindsay wyczuła mój narastający niepokój. Kiedy światła przygasły i podniosła się kurtyna, nachyliła się w moją stronę, szturchnęła mnie łokciem w bok i szepnęła:

– Nikt nie przyszedł tu z twojego powodu. Ludzie chcą po prostu obejrzeć spektakl.

Spędziliśmy też sporo czasu w moskiewskich muzeach. Galeria Trietiakowska ma w zbiorach jedną z największych na świecie kolekcji prawosławnych ikon. Malarze ikon tworzyli na zlecenie Kościoła i nie sygnowali swoich prac. Tradycja i czasy, w których powstawały te dzieła, nie sprzyjały uznawaniu osiągnięć jednostki. Kiedy Lindsay i ja zatrzymaliśmy się przed jedną z ikon, podeszła do nas nastoletnia turystka. Wcześniej zdarzało się już, że rozpoznawano mnie w miejscach publicznych, ale tym razem byłem w towarzystwie Lindsay – to zwiększało ryzyko trafienia na nagłówki gazet. Nastolatka, mówiąca po angielsku z niemieckim akcentem, zapytała, czy może zrobić sobie z nami selfie. Sam nie wiem, dlaczego bez wahania wyraziłem zgodę – być może sprawił to nieśmiały i uprzejmy sposób, w jaki młoda Niemka zadała pytanie, a może była to zasługa obecności Lindsay i tego, że udzieliło mi się jej pogodne

i wyrozumiałe podejście do ludzi. Lindsay uśmiechnęła się, a stojąca między nami dziewczyna wyciągnęła telefon i zrobiła zdjęcie. Zanim odeszła, przekazała mi jeszcze kilka miłych słów wsparcia.

Chwilę później wyciągnąłem Lindsay z muzeum. Przestraszyłem się, że nastolatka zamieści zdjęcie w mediach społecznościowych – gdyby tak się stało, w ciągu kilku minut moglibyśmy znaleźć się w centrum niepożądanej uwagi. Dziś jest mi głupio, kiedy myślę o swojej reakcji. Przez pewien czas sprawdzałem nerwowo, czy nasze zdjęcie nie pojawi się gdzieś w internecie. Ale nie pojawiło się – ani tamtego dnia, ani nazajutrz. O ile wiem, nigdy nie zostało udostępnione publicznie; pozostało prywatną pamiątką tamtego przypadkowego spotkania.

Za każdym razem, gdy wychodzę z domu, staram się zmieniać nieco wygląd. Czasem zgolę zarost, czasami nałożę okulary inne niż zwykle. Nie lubiłem zimna, dopóki nie zdałem sobie sprawy, że założenie czapki i szalika pozwala ukryć tożsamość i nie rzucać się w oczy. Staram się zmieniać rytm i tempo kroków, a kiedy przechodzę przez jezdnię, wbrew mądrym radom mojej mamy nigdy nie patrzę w kierunku nadjeżdżających samochodów, dzięki czemu nigdy nie zostałem uchwycony w obiektywie samochodowych kamer, z których korzystają niemal wszyscy rosyjscy kierowcy. Mijając budynki wyposażone w monitoring, zawsze opuszczam głowę, żeby mój zarejestrowany wizerunek nie przypominał tego, jaki wszyscy znają ze zdjęć dostępnych w internecie. Początkowo obawiałem się podróżować autobusami i metrem, ale szybko uświadomiłem sobie, że w dzisiejszych czasach wszyscy zbyt pilnie wpatrują się w ekrany smartfonów, żeby zatrzymać na mnie wzrok. Kiedy zamawiam taksówkę, nigdy nie wsiadam do niej pod domem, tylko na jednym z pobliskich

przystanków autobusowych, a następnie wysiadam w miejscu oddalonym o kilka budynków od celu podróży.

Dziś wybrałem się na długą przechadzkę po tym ogromnym, dziwnym mieście w poszukiwaniu kwiatów. Czerwonych róż, białych róż, a nawet niebieskich bratków. Wszystkich, jakie tylko zdołam znaleźć. Nie znam ich rosyjskich nazw, więc po prostu chrząkam i pokazuję je sprzedawcom palcem.

Lindsay mówi po rosyjsku lepiej ode mnie. Jest też bardziej niż ja skłonna do śmiechu, cierpliwsza, bardziej wielkoduszna i miła.

Dziś wieczorem obchodzimy rocznicę. Lindsay przeprowadziła się do Moskwy przed trzema laty, a dokładnie dwa lata temu wzięliśmy ślub.

---

* ACLU – Amerykański Związek Swobód Obywatelskich (patrz tutaj).

Podziękowania|

Nigdy nie czułem się tak samotny jak w maju 2013 roku, gdy w pokoju hotelowym w Hongkongu zastanawiałem się, czy dziennikarze przyjadą się ze mną spotkać. Teraz, sześć lat później, znajduję się już w całkowicie odmiennej sytuacji, przyjęty do niezwykłego i stale powiększającego się ogólnoświatowego bractwa dziennikarzy, prawników, specjalistów z dziedziny nowych technologii i obrońców praw człowieka; wobec niego mam ogromny dług. Na końcu autor zazwyczaj dziękuje osobom, dzięki którym książka mogła powstać, i oczywiście zamierzam to zrobić. Biorąc jednak pod uwagę okoliczności, nie do wybaczenia byłoby, gdybym nie podziękował przede wszystkim tym, dzięki którym wciąż mogę żyć – ludziom stającym w obronie mojej wolności, a przede wszystkim niestrudzenie i bezinteresownie działającym na rzecz ochrony naszych otwartych społeczeństw i otwartych technologii; one nas połączyły i nadal wszystkich łączą.

Przez ostatnich dziewięć miesięcy uczyłem się pisać pod okiem Joshuy Cohena, to on pomógł przekształcić moje chaotyczne wspomnienia i zwięzłe manifesty w książkę, z której, mam nadzieję, może być dumny.

Chris Parris-Lamb okazał się bystrym i cierpliwym agentem, a Sam Nicholson swoją redakcją nadał tekstowi przejrzystość i zapewnił mi wsparcie, podobnie jak cały zespół w wydawnictwie Metropolitan, począwszy od Gillian Blake przez Sarę Bershtel i Rivę Hocherman po Grigory’ego Tovbisa.

Sukces tego zespołu jest świadectwem talentów jego członków oraz założyciela – Bena Wiznera, mojego prawnika; z dumą mogę go nazwać również swoim przyjacielem.

Równocześnie pragnę podziękować międzynarodowemu zespołowi prawników, który niezmordowanie pracuje, żeby umożliwić mi pozostawanie na wolności. Dziękuję również Anthony'emu Romero, dyrektorowi ACLU; to on zajął się moją sprawą w czasie, kiedy pociągało to z sobą poważne polityczne ryzyko dla jego organizacji. Dziękuję także innym pracownikom ACLU pomagającym mi przez te wszystkie lata, w tym Bennettowi Steinowi, Nicoli Morrow, Noi Yachot i Danielowi Kahnowi Gillmorowi.

Jestem też wdzięczny Bobowi Walkerowi, Jan Tavitian i ich zespołowi z American Program Bureau – umożliwili mi zarabianie na życie poprzez rozpowszechnianie mojego przesłania wśród nowych odbiorców na całym świecie.

Trevor Timm oraz inni koledzy z rady dyrektorów Fundacji na Rzecz Wolności Prasy zapewnili mi przestrzeń i zasoby, żebym mógł powrócić do prawdziwej pasji i wykorzystywać własne umiejętności techniczne dla dobra ogółu. Jestem szczególnie wdzięczny Emmanuelowi Moralesowi, byłemu dyrektorowi do spraw operacyjnych FPF, oraz obecnemu członkowi rady Danielowi Ellsbergowi, który stał się dla świata wzorcem prawości, a mnie obdarzył ciepłą i szczerą przyjaźnią.

Ta książka została napisana z wykorzystaniem wolnego i otwartego oprogramowania. Pragnę podziękować Qubes Project, Tor Project i Free Software Foundation.

Po raz pierwszy zrozumiałem, co to znaczy mieć termin oddania tekstu dzięki moim mistrzom: Glennowi Greenwaldowi, Laurze Poitras, Ewenowi MacAskillowi i Bartowi Gellmanowi. Ich profesjonalizm opiera się na

żarliwej rzetelności. Po tym, jak sam zredagowałem swój tekst, jeszcze bardziej doceniam redaktorów z ich strony, którzy nie dali się onieśmielić i podjęli ryzyko, które nadało znaczenie wyznawanym przez nich zasadom.

Najgłębszą wdzięczność rezerwuję dla Sarah Harrison.

A moje serce należy do rodziny – do ojca Lona, matki Wendy, i wspaniałej siostry Jessiki.

Tę książkę mogę zakończyć tylko w jeden sposób, a mianowicie tak, jak ją zacząłem: dedykacją dla Lindsay, której miłość zmienia wygnanie w życie.